TURING

著名安全专家解密社会工程手法的权威著作
社会工程专家的精彩故事令你瞠目结舌
众多专业人士强力推荐，亚马逊读者一致好评

Social Engineering: The Art of Human Hacking

# 社会工程

[美] Christopher Hadnagy 著　陆道宏　杜娟　邱璟　译

## 安全体系中的人性漏洞



人民邮电出版社
POSTS & TELECOM PRESS

# 数字版权声明

图灵社区的电子书没有采用专有客户端，您可以在任意设备上，用自己喜欢的浏览器和PDF阅读器进行阅读。

但您购买的电子书仅供您个人使用，未经授权，不得进行传播。

我们愿意相信读者具有这样的良知和觉悟，与我们共同保护知识产权。

如果购买者有侵权行为，我们可能对该用户实施包括但不限于关闭该帐号等维权措施，并可能追究法律责任。

**Christopher Hadnagy** 世界上第一个社会工程框架（www.social-engineer.org）的主要开发者。与BackTrack（www.backtrack-linux.org）安全团队一起参与了各种类型的安全项目，有16年以上的安全和信息技术实践经验。他也是主动式安全（Offensive Security）渗透测试小组的培训师和首席社会工程专家。

**陆道宏** 1995年毕业于华东理工大学计算机与科学系，获硕士学位，长期从事信息安全与计算机取证研究和开发工作。2004年，合伙创建盘石软件（上海）有限公司，领导开发了盘石计算机现场取证系统（SafeImager）、盘石速影网站猎手（SafeSite）等系列计算机取证专业工具。

**杜娟** 毕业于华东政法大学刑事司法学院计算机科学与技术专业。现就职于盘石软件（上海）有限公司计算机司法鉴定所，任职期间完成多起电子物证案件的鉴定，主导鉴定实验室通过国家认可委CNAS认证认可，为多个省部级单位做过电子数据取证的专业技术培训。

**邱璟** 计算机取证行业从事者，信息安全、计算机犯罪研究、计算机司法鉴定研究爱好者。毕业于华东政法大学刑事司法学院计算机科学与技术专业。现就职于盘石软件（上海）有限公司，专业从事计算机取证调查工作。

Social Engineering: The Art of Human Hacking

# 社会工程

[美] Christopher Hadnagy 著 陆道宏 杜娟 邱璟 译

## 安全体系中的人性漏洞



人民邮电出版社
北 京

图书在版编目（C I P）数据

社会工程 ：安全体系中的人性漏洞 / (美) 海德纳吉 (Hadnagy,C.) 著 ; 陆道宏, 杜娟, 邱璟译. -- 北京: 人民邮电出版社, 2013.12
书名原文: Social engineering:the art of human hacking
ISBN 978-7-115-33538-8

Ⅰ. ①社… Ⅱ. ①海… ②陆… ③杜… ④邱… Ⅲ. ①信息安全 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2013)第263458号

## 内 容 提 要

本书首次从技术层面剖析和解密社会工程手法，从攻击者的视角详细介绍了社会工程的所有方面，包括诱导、伪装、心理影响和人际操纵等，并通过凯文・米特尼克等社会工程大师的真实故事和案例加以阐释，探讨了社会工程的奥秘。主要内容包括黑客、间谍和骗子所使用的欺骗手法，以及防止社会工程威胁的关键步骤。

本书适用于社会工程师、对社会工程及信息安全感兴趣的人。

◆ 著　　　[美] Christopher Hadnagy
译　　　陆道宏　杜　娟　邱　璟
责任编辑　李　瑛
执行编辑　卢秀丽
责任印制　焦志炜

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京　　　　　　印刷

◆ 开本：800×1000　1/16
印张：18.25
字数：430千字　　　　2013年 12 月第 1 版
印数：1 – 3 500册　　　2013年 12 月北京第 1 次印刷
著作权合同登记号　　图字：01-2012- 3282号

定价：59.00元

**读者服务热线：(010)51095186转600　印装质量热线：(010)81055316**

**反盗版热线：(010)81055315**

**广告经营许可证：京崇工商广字第 0021 号**

# 版 权 声 明

谨以此书献给我美丽的妻子和可爱的家人。如果没有你们，我根本无法完成本书的写作。Mati，我对你的感激之情无以言表。

# 序

安全对内外部双方来说都是个难题。从内部来看，我们需要舒适感和安全感；从外部来看，窃贼、黑客和蓄意破坏者在不断寻找突破口。大部分人都觉得自己的家是安全的，直到有一天忽然发现自己被锁在了门外。我们的看法就会在刹那间改变，才明白原来安全漏洞是那么明显。

必须置身事外才能全面地理解安全，从本质上来说就是把自己作为一个局外人，尝试用其他方式来进入系统。问题是大部分人因为自信满满而对潜在的问题视而不见，觉得锁很好、门很厚、安全系统很高级，而且还有看门狗，就足以把大部分人“拒之门外”了。

我不属于这部分人。过去10年中，我比历史上任何人设的骗局都要多。我在赌场赢过庄家、伪造过体育赛事、操纵过拍卖、诱骗过他人交出心爱之物，也轻松侵入过几个号称坚不可破的安全系统。

我的工作就是在热门电视节目《骗术真相》（*The Real Hustle*）中曝光窃贼、说谎者和骗子耍的各种伎俩。如果我做了罪犯的话，很可能会变得富有、名噪一时或者难逃一死——也许三者都会发生。人生的大部分时间，我都在研究各种欺骗方式，以便告诉公众他们是多么好骗。

每周，我都和亚历克西斯・康兰（Alexis Conran）一起设局骗人，而被骗的人对于自己身处骗局之中浑然不知。通过隐蔽的摄像头，我们向电视机前的观众演示怎样才能识破同样的骗局。

这种不同寻常的工作使我对罪犯的思维方式有着独到的理解。我逐渐成为一只批着狼皮的羊。以个人经验来看，不管事情看似多么不可能，几乎总会有一种巧妙的、意想不到的解决方法。

举个例子。我曾想证明自己不仅能轻而易举偷取一个女人的钱包，还能让她告诉我信用卡的

提款密码。BBC电视台认为这不可能。当我将这个想法提交给《骗术真相》栏目组，想做一期节目时，BBC台长的批示是“不可能发生”，然后将其退还给我。我们知道这完全可能，因为类似的骗局已在英国各地被报道过，受害者在巧妙的布局下中了计，将密码亲口告诉了盗贼。我们从不同的骗局中提取要素，来切实演示人们到底是怎样受骗上当，并将银行账户的信息和盘托出的。

为了证明我的想法，我们把骗局地点设在本地的一个咖啡厅。咖啡厅位于伦敦牛津大街一个购物广场的顶层。我西装革履地坐在一个相对安静的空桌旁，将公文箱放在桌子上，静候合适的猎物。没过多久，一位女士和朋友一起坐到我的邻桌，她把包放在了旁边的椅子上。也许是个人习惯，她将椅子拉到身边，并一直把手放在包上。

我需要偷取她的包，虽然她的手放在包上而且其朋友就坐在对面，但“悲剧”即将发生。几分钟之后，她的朋友去了洗手间。现在目标只有她一个人，于是我给亚历克斯（Alex）和杰丝（Jess）发了个信号。

亚历克斯和杰丝装成一对夫妻，上前请目标人物帮忙拍个合影，她很高兴能帮上忙。她将手从包上拿开，拿起相机为这对“幸福夫妻”拍照。在她分神的瞬间，我轻松自如地伸手拿起她的包并将其锁进我的公文箱。当亚历克斯和杰丝离开咖啡厅的时候，受害者根本没有注意到椅子已经空了。当亚历克斯从女子的视线中消失之后，他快速奔向停车场。

没过多久，受害者就意识到包不见了。她立即变得很焦躁，她站起身来，疯狂地四处寻找。这正是我们希望发生的情景，我问她是否需要帮忙。

她开始问我有没有看见什么，我告诉她“没有”，安慰她坐下，并让她努力回想包里有哪些东西。她边回忆边说：“一部手机、一些化妆用品、一点现金，还有几张信用卡。”好，进入主题！

在询问完信用卡是哪家银行的后，我便告诉她自己碰巧是那家银行的员工。她真是太“幸运”了！我向她保证不会有事的，但是要马上注销信用卡。我拨通了“客服中心”的号码，事实上是亚历克斯的电话号码，并把电话递给她。她上钩了，接下来就交给亚历克斯，看他怎么让受害人一步步陷入圈套。

亚历克斯在楼下的面包车里，车里的CD播放器播放着我们从网上下载的办公室嘈杂声。他让对方保持冷静，步步为营引诱她入局，然后肯定地告诉她信用卡注销很方便，但为了确认她的身份，需要她在通话手机的键盘上输入信用卡的密码。

我的手机，我的键盘。

接下来就没有任何悬念了。得到密码后，我起身离开了她和她的朋友，径直向门外走去。如果我们是真正的小偷，便可以用她的信用卡和密码在提款机上完成取款/转账等操作，也可以进行各种消费。幸运的是，这只是一档电视节目。当我将包还给她，并告之这只是一场骗局时，她很开心，甚至还感谢我。当然，我只是回答道：“不要感谢我，是我偷了你的包。”

无论系统有多安全，总有方法攻破它。通常，系统中的人是最好欺骗和操纵的。制造恐慌、运用影响力、采用操纵策略和建立信任感等方法都可以让受害者消除戒备。

这个例子可能有些极端，但也证明了，只要使用一点小伎俩，就可以成功实施看似不可能的诈骗。

承认系统有漏洞并且可能被攻破，是让系统更加安全的首要条件。相反，一直坚信系统坚不可摧的人就仿佛蒙着眼睛全速奔跑。社会工程学研究系统中最薄弱的一环——人，以及如何运用人性攻击的技巧攻破看似安全的系统。本书并非黑客指南，因为他们已经知道怎样闯入系统并且每天都在研究新的方法。相反，克里斯·海德纳吉（Chris Hadnagy）揭露了世界上最险恶的黑客、骗子以及社会工程人员的思路和方法，让我们有机会从黑暗的一面，也就是攻击者的视角来看系统安全与防护。

谨记，防御方和进攻方的思维方式是不同的，进攻方会考虑翻、钻、绕甚至穿越等各种方式，以进入为最终目标。就像我经常告诫观众的一样，如果你认为自己不可能被骗，那么你就是我最想骗的那个人。

保罗·威尔逊（Paul Wilson）

2010年10月

# 前言和致谢

几年前，在一次与良师益友马蒂·阿哈罗尼（Mati Aharoni）聊天的过程中，我决定建立网站www. social-engineer.org。在一群杰出人士的共同努力下，这个想法逐渐成熟，最终成立了一个十分神奇的网站。不久以后，将这几年的研究和经验归纳成书的想法也随之浮现。当我提议著书时，众人随即表示大力支持。在此，要特别感谢那些为本书的问世作出巨大贡献的人们。

从年轻时起，我就一直对操控别人特别感兴趣。当然不是通过卑鄙的方法，我只是对取得意外收获或者将不可能变为可能很感兴趣。有一次，我和一位好友兼商业伙伴参加在纽约贾维茨会议中心举办的技术会议。一家大型公司租用了施瓦茨玩具城来举办一场私人派对。只有持有邀请函的客人才能进入该派对，且派对邀请的都是惠普、微软等知名企业的首席执行官和高层管理人员，而我们俩只是两个小人物。朋友对我说："如果能参加那个派对，就酷毙了！"

我平淡地回应道："我们为什么不能参加呢?"当时我暗想：只要找到正确的方式，我们就可以参加这个派对。所以我走近负责签到的女工作人员，和她们交谈了几分钟。就在这个时候，Linux内核的创始人林纳斯·托瓦兹（Linus Torvalds）走了过来。我从其中的一个验票处拿起一个带有微软标志的长毛绒玩具，然后转向林纳斯，开玩笑地说："嘿，你想在我的微软玩具上签名吗？"

他大笑，扬起票说："不错嘛，年轻人，派对上见。"

我转向负责验收邀请函的女工作人员，便得到了两张该派对的邀请函。

后来我才开始对类似的事情进行分析，并将其称为"海德纳吉效应"。听起来很有趣，但我

发现在自己身上发生的很多事情，与其说是运气好或者命运使然，倒不如说是我知道如何在正确的时间做正确的事。

这并不意味着在前进的道路上我不需要努力工作和他人的帮助。我可爱的妻子正是我的缪斯女神。近20年来，你一直支持我的想法和努力，你是我最好的朋友、我的知己、我的支柱。没有你，就不会有今天的我。此外，你还为我带来了这个世界上最美丽的两个孩子。儿子和女儿是我继续从事这一切的强大动力。如果我的所作所为能使他们更安全一些，或者能够教导他们如何才能保障自身的安全，那就值得了。

我的儿子和女儿，对于你们给予我的支持、爱和动力，再多的语言也不足以表达我的谢意。希望我的小王子和小公主不用和那些心怀鬼胎的人打交道，但我知道那是不可能的。因此，希望本书中的信息多少能使你们俩更安全些。

保罗（Paul，网名rAWjAW），感谢你对网站的所有支持。作为“维基大师”，你经过数千小时的努力工作，带给我们一个供全世界使用的极佳的网站。“你可以回家休息了！”我对你的谢意溢于言表。汤姆（Tom，网名DigIp）的完美创造力更是锦上添花，是你们把网站塑造成了一件艺术品。

卡罗尔（Carol），Wiley出版社的编辑，辛辛苦苦地组织和跟进各个零散的进程。你凭借卓尔不凡的工作能力将一群人凝聚到这个伟大的团队中来，并使得我们的想法成为现实。谨在此表示我的谢意。

布莱恩（Brian），说实话，当这一切结束时，我会想念你的。在共事的几个月里，我十分期待你在编辑会议中带给我们的那些智慧的火花。你真诚、坦率的建议和忠告使得本书更为出彩。

同样，我还要感谢吉姆（Jim，网名 Elwood）。如果没有你，许多发生在social-engineer.org网站上以及本书中的事，甚至近几年我生活中的一些事，都不会成为现实。谢谢你使我保持谦逊和严谨。你不间断的核查有助于我集中注意力，使我所扮演的众多角色得到平衡。谢谢你。

利兹（Liz），大约12年前，你就建议我写一本书。我确信你当时所想的和现在不一样，幸而书已付梓。你帮助我度过了相对黑暗的一段时期。谢谢你，我爱你。

马蒂（Mati），我的导师，我的兄弟，若没有你，我会是什么样子呢？马蒂，你是我真正的导师和兄弟。我衷心感谢你给予我写作本书以及创建www.social-engineer.org网站的信心。不仅如此，你不断提供的建议和指导已经融入到本书的创作中，让我实现了自我超越。

你与BackTrack团队以及www.offensive-security.com团队的支持超出了我的预计。谢谢你们帮助我权衡利弊，实现主次有序。我的兄弟，特别感谢你，感谢你的理性，也感谢你在我沮丧的日子里带给我希望。衷心地谢谢你。

这里提到的每个人都在某些方面促成了本书。在他们的帮助、支持和厚爱下，我才能自豪地

在本书的封面署上自己的名字。还有其他支持网站、渠道和我们研究的人，谢谢你们。

编写本书时，它对我产生了极为深远的影响，希望你阅读本书时也能有同样的感受。

爱因斯坦曾经说过：“信息并非知识。”这是一个伟大的观点。只是简单地阅读本书并不会将知识植入你的生命中。应用书中的原则，实践书中的内容，使这些信息成为日常生活的一部分。只有这么做，这些知识才能够真正起作用。

克里斯托弗·海德纳吉（Christopher Hadnagy）

2010年10月

# 目　　录

# 第 1 章
# 社会工程学初探

知己知彼，百战不殆。
——孙子

社会工程[1]（Social Engineering）在很大程度上被人们误解了，从而导致人们对其定义和工作方式有很多不同的观点。有人简单地将社会工程视为撒谎，可以骗得免费的比萨或骗财骗色等；有人将其归类为罪犯或骗子的工具；也有人将其划到科学的范畴，认为其理论可以分门别类或采用数学公式加以研究；还有人将其视为长久失传的神秘技艺，掌握了社会工程学，从业者就能像魔术师那样制造强大的思维幻觉。

无论你的想法如何，你都可以从本书中获益。每个人每天都会在各种情况下使用社会工程的方法。小孩利用它来得到糖果，雇员利用它来得到晋升。大到政府部门的运作，小到公司的市场行为，或多或少都有社会工程的影子。不过罪犯和骗子之流也利用社会工程达到窃取他人信息和犯罪的目的。与任何工具一样，社会工程无好坏之分，它仅仅是一种多用途的工具。

下面这些问题有助于进一步理解本书的观点。

- 你需要尽可能确保公司安全吗？
- 你是每日阅读最新安全信息的人吗？
- 你是测试客户系统安全的专业渗透测试人员吗？
- 你是主修信息技术专业的大学生吗？

① 中国大陆的书籍和文章中普遍采用的译法是“社会工程”，台湾地区更多翻译成“社交工程”。本书一律依照大陆的译法。——译者注

- 你是需要新的、更好的社会工程观念以应用到实践中的社会工程人员（Social Engineer）[①]吗？
- 你是惧怕欺诈和身份盗用的消费者吗？

不管你是上述哪一类人，本书所包含的内容都会在应用社会工程技巧方面开阔你的视野。你将会了解社会工程的黑暗世界，懂得“坏人”是怎样使用社会工程的方法占据先机的，从而学会有效防御社会工程的攻击。

请注意，本书并非为弱者所作。它会带你领略社会的黑暗面，那里是“坏蛋”及恶意黑客的世界。本书将揭示并深入研究间谍和骗子所使用的社会工程技巧，评述类似007电影中的战术和工具，还将介绍日常情境是怎样成为复杂的社会工程场景的，最后将披露专业社会工程人员甚至是专业罪犯所使用的技巧和花招。

有人曾问我为何愿意公开这些信息，答案很简单：“坏人”不会由于契约限制或道德约束停止犯罪，他们不会因为一次失败就停止尝试，恶意黑客也不会因为公司不喜欢服务器被入侵就自动走开。事实是社会工程、员工被骗和网络欺诈的戏码每天都在上演。在软件公司不断加固程序的同时，黑客和恶意社会工程人员将目光转向基础设施中最薄弱的一环——人。他们的动机只是获得投资回报率，没脸没皮的小黑客会为一个简单的攻击花费上百个小时，而掌握社会工程技术的高级黑客只需一小时甚至更短的时间。

结果是没有绝对的安全，除非你拔掉所有电源并躲进深山老林，但是这种方法操作性不强，也不好玩。本书将讨论如何了解攻击、意识到攻击，并且防御攻击。我的信条是“学而知安全”。当前，社会工程攻击和账户盗用现象日益严重，掌握知识是确保安全的唯一有效方法。卡巴斯基实验室是开发病毒防护软件的顶尖厂商之一，他们估计2009年的社交网络中有10万多个恶意软件样本传播。在最近的一份报告中，卡巴斯基估计“针对社交网络的攻击的成功率是其他形式攻击的10倍”。

俗语“知识就是力量”用在这里很恰当。用户和企业对社会工程攻击的危险和威胁了解越多，理解越深入，对常见攻击场景越熟悉，也就越容易防御、减轻甚至完全阻止这类攻击。这就是知识的力量所在。

## 1.1　为何本书很重要

市场上有很多关于安全、黑客、渗透测试甚至社会工程学的书籍，其中有不少书为读者提供了很有价值的信息和提示。然而，即使有了这些信息，还是需要一本高阶的社会工程学书籍，来从攻击者的角度详细讲解社会工程攻击。本书并非简单罗列精彩的故事、漂亮的攻击以及疯狂的想法，而是讲述世界上第一个社会工程框架，详细分析成为一名优秀社会工程人员所需具备的基

① Social Engineer，指利用社会工程技术获益的人员，本书统一翻译成“社会工程人员”。——译者注

础要素，并就如何使用社会工程的技巧提供实用的建议，以提高读者测试系统中最薄弱的环节（人）的能力。

### 1.1.1 本书框架

本书以独特的方法研究社会工程学，其架构和www.social-engineer.org/framework网站中深入彻底的社会工程框架很类似。该框架列出了要成为一名优秀的社会工程人员，需要拥有的工具和掌握的技能（实体、心理和个性方面的）。

本书采用“解析加演示”的写作方法，首先讲解一个课题的原理，随后进行定义、解释和深入分析，最后使用真实故事或案例来演示其应用。本书并不单纯讲精巧的骗局故事，而是要写成一本了解社会工程学中黑暗世界的手册和指南。

全书提供了很多网络链接，可以了解更多的故事、实例账户、安全工具以及其他相关话题，还有很多实用练习，有助于你进一步掌握社会工程框架，同时提高日常沟通的技能。

上述内容对安全专员更加适用。我希望在阅读本书的时候，你能意识到安全并非“业余”工作，不可小视。罪犯和恶意社会工程人员越来越猖獗，对企业和个人生活的攻击在不断增多。自然地，人们也需要得到保护，这也是个人防护软件和设备热卖的原因。虽然这些产品很重要，但最好的防护是掌握知识。减弱攻击影响的唯一正确方法是知晓其存在、掌握其原理并懂得攻击者的思维过程和心理。

掌握这些知识并了解恶意黑客的思维方式，就像拥有了一盏明灯，可以照耀那曾经昏暗的角落，让你看清潜伏的“恶意攻击者”。若能提前知晓攻击方法，就可以采取预防措施，使公司或者个人事务免受攻击。

当然，我依然认为没有绝对的安全，二者并非自相矛盾。即使是重重防护的高级机密，也会而且确实曾经被轻易拿下过。

社会工程网站www.social-engineer.org/resources/book/TopSecretStolen.htm上有一个故事，摘自加拿大渥太华的一份报纸。这个故事很有趣，原因在于一些文档落入了错误的人手中。这些并非一般的文档，而是高度机密的国防文档，其中包括加拿大特伦顿军事基地安全隔离墙的位置信息、加拿大联合响应部队的平面图等。这些文档是怎么得到的？很简单，文档被丢到垃圾桶中，有人从垃圾箱里翻了出来。只要翻翻垃圾箱就能找到一个国家的绝密安全信息！

简单而致命的攻击每天都在发生，所以人们需要掌握知识、改变密码策略、改变远程服务器的访问方式，还需要在面试、交付、雇用和解聘员工方面改变思路。如不具备知识，也便没有改变的动力。

2003年，计算机安全研究所和FBI的一项联合调查发现，77%的被调查公司声称员工报复是

安全入侵事件的主因。赛门铁克公司的数据丢失防护部门Vontu（http://go.symantec.com/vontu/）声称，每500封邮件中就有一封包含机密数据。调查报告中包含如下一些信息（引自http://financialservices.house.gov/media/pdf/062403ja.pdf）。

- 62%的报道事件中存在客户身份被盗的风险；
- 66%的受访者认为他们的同事而非黑客会给客户隐私带来最大的风险，只有10%的受访者认为黑客是最大的威胁；
- 46%的受访者声称，员工从公司数据库中移除敏感信息是件“很简单”甚至是“轻而易举”的事情；
- 32%也就是约1/3的受访者不清楚公司保护客户数据的内部策略。

这些就是令人吃惊且头痛的统计数据。

后续章节会详细讨论这些数字。这些数字显示了安全处理中的严重缺陷。必须未雨绸缪，在被入侵之前掌握安全知识，才能做出改变，从而避免不必要的损耗、痛苦和经济损失。

孙子曰：“知己知彼，百战不殆。”真是至理名言！但只是“知”尚且不够，知行合一才是智慧所在。

本书作为社会攻击、社会操纵和社会工程的手册或指南使用最为有效。

### 1.1.2　本书内容

本书涵盖了专业和恶意社会工程人员所使用的工具和技能等各个方面。每章会深入探讨其中一项技能，介绍如何利用、提高和完善它。

下一节将定义社会工程学及其在当前社会中所扮演的角色，以及社会工程攻击的不同类型，包括社会工程在日常生活其他领域中的非恶意使用。同时还会讨论社会工程人员怎样利用社会工程框架来计划审计工作或提高自身技能。

第2章是实战课程的正式开始。信息收集是每一次社会工程实战的基础。社会工程人员的箴言是：“我所能做的一切均基于所收集的信息。”社会工程人员可能掌握各种技能，但是如果他不了解目标，没有勾画出所有的细节，那么等待他的只能是失败。信息收集是每一次社会工程实践的关键，虽然个人技能和迅速反应的能力也能使你摆脱棘手的情况，但一般情况下，掌握的信息越多，成功的机会也就越大。

我在第2章中会回答以下问题。

- 社会工程人员使用哪些信息来源？
- 什么样的信息是有用的？
- 社会工程人员怎样收集和组织信息？

- 社会工程人员要多专业？
- 掌握多少信息才够？

在分析了信息收集之后，第2章还会讨论交流模型，这两者是紧密相连的。首先会介绍交流模型的定义及其发展，随后会讨论怎样开发和使用一个正确的交流模型，还会简要介绍社会工程人员怎样使用该模型攻击目标并从中受益。

第3章探讨的是诱导，这是社会工程框架中的下一步。本章深入探讨了怎样通过提问来获取信息、口令，并详细了解目标及其公司的信息。你将学习到什么是好的、正确的诱导方式，以及诱导计划的制定是何等重要。

第3章还涵盖一个重要的话题，即如何使用信息来诱导目标的思维，从而让目标轻易接受你的问题。通过本章的学习，你将清楚地了解成为一个出色的“诱导者”有多么重要，以及如何在安全实践及日常生活中使用该技能。

第4章很重要，它讨论的是伪装，这是很多社会工程人员的关键技能之一。伪装涉及选定社会工程人员在攻击公司时所扮演的角色。社会工程人员可以伪装成客户、厂商、技术支持人员、新进员工，甚至是其他同样现实且可信的角色。伪装不仅需要一个故事背景，而且要角色扮演，要掌握扮演对象的眼神以及说话和行走等行为方式，要确定该人可能具备的知识和工具，了解其方方面面。这样当你以他的身份接近目标时，你*就是*他，而不仅仅是在演戏。本章会回答如下问题。

- 什么是伪装？
- 怎样选定伪装对象？
- 成功伪装的原则是什么？
- 社会工程人员怎样计划并执行完美的伪装？

框架中的下一步会占用大量的篇幅，而且必须从社会工程人员的角度来进行讨论。第5章讨论的是一些开放式话题，包括*眼神的暗示*等。例如，专家对眼神暗示有哪些不同观点？社会工程人员怎样使用眼神暗示？本章还会讨论有趣的微表情，以及它对社会工程的启示。

本章主要是研究型的内容，会回答如下问题。

- 安全领域可能会使用微表情吗？
- 怎样使用微表情？
- 微表情有什么好处？
- 人们可以训练自己从而掌握微表情吗？
- 在训练之后，微表情可以带来哪些信息？

第5章最具争议的话题可能是*神经语言程序学*（Neurolinguistic Programming，NLP）。很多人不确定什么是神经语言程序学以及怎样使用它，第5章简要介绍了NLP的历史及其备受争议的原

因，你可以自己决定社会工程中是否可以用到它。

第5章还会讨论面对面或电话沟通时社会工程的一个关键方面：怎样提出恰当的问题、倾听反馈及追加更多问题。司法人员多年来一直使用审问的方式来引导罪犯认罪及破解疑难案件。这部分内容也是对第3章所述知识的应用。

此外，第5章还会讨论怎样瞬间建立亲密关系，该技巧在生活中亦可应用。本章结尾是我个人的研究结果——“思维缓冲区溢出”，其含义是人类的思维与黑客每天破解的软件有很多相似之处。采用特定的方式，技术娴熟的社会工程人员可以溢出人类的思维并注入他们想要的命令。

与黑客通过溢出程序操纵软件来执行代码相似，人类思维也会接受特定的指令，本质上就是“溢出”目标的思维从而插入定制的指令。第5章是激动人心的一章，将介绍如何使用简单的技术掌握人们的思考方式。

很多人一生都在研究和证明哪些因素可能会影响人们。影响力是一个强大的工具，具有很多层面。第6章讨论说服的基础知识，本章中所阐释的原则将会引导你成为极具说服力的大师。

第6章首先简要讨论当前存在的不同类型的说服方式，并且提供实例来强化其在社会工程中的不同应用。

随后会探讨当前的另一热门话题——框架（Framing）。对于框架的使用存在很多不同的观点，本书展示了生活中的一些实例。通过对每个实例的剖析，你可以学到一些经验教训并练习怎样改变自己的框架，及作为社会工程人员在日常生活中怎样使用框架。

另一个社会工程中的重要主题是操纵。

- 操纵的目的何在？
- 操纵者的动机是什么？
- 社会工程中怎样应用操纵？

第6章展示了社会工程人员所必须掌握的关于操纵的所有内容，以及怎样成功地应用这些技巧。

第7章介绍使社会工程审计更为成功的工具。从隐藏的摄像头等物理工具到软件驱动的信息收集工具，每一节都介绍了社会工程人员可使用的经过测试和检验的工具。

在对社会工程框架有足够的了解之后，第8章将讨论一些实际生活中的案例。我选择了世界知名社会工程专家凯文·米特尼克（Kevin Mitnick）的两段精彩故事。通过分析和解读，为读者提炼这些案例中可供学习之处，并与社会工程框架中的方法相对照，还会将这些攻击载体与当前的实际应用相关联。我也会讨论一些个人的案例并进行分析。

社会工程指南如果不讨论攻击的削弱和防御方法就不能算是完整的，第9章会提供这方面的

信息。我会就缓解攻击方面的一些常见问题给出答案，并且就巩固安全和防御恶意攻击给出不错的建议。

前面只是对本书内容的简要概述，我真诚地希望你喜欢阅读本书，就像我享受写作的过程一样。我对社会工程学充满激情。我相信总有一些人，通过学习和挖掘一些与生俱来的潜质，会成为伟大的社会工程人员。我也相信，只要投入足够的时间和精力，任何人都可以通过对社会工程学的学习和不断的练习，成为一名专业的社会工程人员。

本书中的基本原理并不新颖，你也不会看到令人震惊的、会改变世界的技术。这里没有万能神药。事实上，人们早就拥有这方面的知识。本书只是将所有相关技巧组织在一起，以便读者明确方向，练习这些技巧，并认识到日常生活中的应用场景。所有信息都可以帮助读者正确理解各个章节所讨论的内容。

让我们从最基础的问题开始，先来回答“什么是社会工程”。

## 1.2　社会工程概述

什么是社会工程？

我曾就此问题询问一组安全爱好者，得到的答案令我非常惊讶。

- “社会工程是欺骗别人以获取信息。”
- “社会工程就是做一个好演员。”
- “社会工程是知道怎样免费获得东西。”

维基百科的定义是：“操纵他人采取特定行动或者泄漏机密信息的行为。它与骗局或欺骗类似，故该词常用于指代欺诈或诈骗，以达到收集信息、欺诈和访问计算机系统的目的，大部分情况下攻击者与受害者不会有面对面的接触。”

虽然常被冠以恶名，从“免费比萨”、“免费咖啡”及“把妹”等就可见一斑，但社会工程学实际上触及生活中的很多方面。

韦氏字典对社会（Social）的定义是“社区中属于或与生活、福利以及人际关系有关的”，对工程（Engineering）的定义则是“对物理、化学等纯粹科学进行实际应用的艺术或科学，如构建发动机、桥梁、建筑物、矿井、船只和化工厂等，技术或制作精巧的发明；机械控制”。

将这两个定义进行组合，很容易就可以发现社会工程学是一门艺术或者说得更好听是一门科学，它有技巧地操纵人们在生活中的某些方面采取某种行动。

这个定义将社会工程人员的活动范围扩大到生活的各个方面。小孩使用社会工程从父母处得

到他们想要的东西，老师采用社会工程与学生互动，医生、律师或心理学家运用社会工程从病人和客户那里得到信息。当然，司法部门也在使用，人们约会时也使用。事实上，从婴儿到政治家，每个人在交往活动中都在运用社会工程。

我对该定义进行了扩展，认为社会工程的真正定义是：一种操纵他人采取特定行动的行为，该行动不一定符合“目标人”的最佳利益，其结果包括获取信息、取得访问权限或让目标采取特定的行动。

举例来说，医生、心理学家及临床医学家通常使用社会工程的一些因素“操纵”病人，使其采取对病人有益的行动。相反，骗子使用社会工程的某些因素说服目标，使其采取给目标自身带来损失的行动。虽然两者的最终结果迥异，但其中的方法却很类似。心理学家使用一系列精心设计的问题，帮助病人得出必须改变的结论。类似地，骗子使用精心构造的问题将目标置于危险的境地。

虽然这两个例子都是社会工程的最真实形式，但是具有不同的目标和结果。社会工程不能仅仅定义为欺骗、撒谎或角色扮演。在我与克里斯·尼克森[Chris Nickerson，电视剧《老虎小组》（*Tiger Team*）中的知名社会工程人员]的一次交谈中，他说：“真正的社会工程不仅是以为自己在扮演角色，而且在那个时刻，你*就是*那个人，你就是那个角色，你的生活就是那样的。”

社会工程不是任何一种独立的活动，而是由框架中提到的各种技巧组合形成的活动、技巧和科学。同样，一种美食也不会仅有一种成分，而是精心组合、调配及添加多种配料而成的。社会工程就像烹调，而一个优秀的社会工程人员就像是主厨。使用少量的诱因，稍加操纵和伪装，就能成为一名完美的社会工程人员。

当然，本书会讨论其中的一些方面，但重点是你能从执法人员、政治家、心理学家甚至儿童身上学到什么，以提高你在审计及加强自身安全方面的能力。对儿童轻而易举就能“操纵”父母的行为进行分析，可以就人们的思维方式给社会工程人员以启示；分析心理学家怎样组织问题，可帮助我们理解什么能让人放松；分析执法人员成功审问的方法，可以了解如何从目标身上获取信息；分析政府部门和政治家如何传达消息以取得最大影响力，我们能知道哪些行为可行；分析演员怎样进入角色，会令你进入角色扮演的精彩世界；通过研究和分析微表情和说服方面的前沿知识，可以学习其在社会工程中的应用；通过分析世界上最出色的销售人员和谈判专家的动机，可以了解怎样建立密切的关系，使对方放松警惕，从而达成目标。

通过对反面示例（骗子及小偷等）的研究和分析，你会看到他们怎样综合应用这些技巧影响他人，让人们做出一些自己都想不到的事情。

将这些知识和开锁匠、使用隐秘摄像机的间谍、专业信息收集人员的技巧相结合，你会成为一个才华出众的社会工程人员。

一次行动中不需要使用所有这些技巧，你也不可能掌握所有的技巧。通过理解这些技巧的用

法以及使用时间，任何人都可以掌握社会工程学。确实，有些人天生就有这方面的才能，例如凯文·米特尼克，他可以说服任何人做任何事。小弗兰克·阿巴奈尔（Frank Abagnale, Jr.）[①]天生就具有欺骗别人、令别人相信他所扮演的角色的能力。维克多·拉斯体格（Victor Lustig）的所作所为更让人难以置信，他使一些人相信他有权销售埃菲尔铁塔[②]，其最厉害的一次当属欺骗了黑帮老大艾尔·卡彭（Al Capone）。

这些社会工程专家和其他类似人员似乎天生就具有这方面的能力，也拥有无畏的精神，使得他们可以尝试大部分人想都不敢想的事情。不过，今天的恶意黑客在不断提高操纵他人的能力，恶意的社会工程攻击在不断增多。黑暗阅读（DardReading）网站的一篇文章（网址是www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=226200272）中说道，一次数据入侵事件会给相关公司带来100万到5300万美元的损失。网站引用的是波耐蒙（Ponemon）研究所的结果："波耐蒙发现对网站的攻击、恶意代码和恶意的内部人员是最具破坏性的攻击形式。平均每年每个企业因网络犯罪所遭受的损失中，有90%以上是由这三种攻击造成的。一次网站攻击造成的损失是143 209美元，恶意代码造成的损失是124 083美元，恶意内部人员造成的损失是100 300美元。"恶意内部人员进入前三名意味着商业人士需要更加关注来自恶意社会工程方面的威胁，包括来自员工的威胁。

如果人们掌握相关的知识，则很多此类攻击就可以避免，因为人们可以根据所掌握的知识采取行动。有时了解恶意攻击者的思维和行为方式，就能对很多事情作出判断。

举一个简单的例子。近期一位好友告诉我，她很担心金融账户被入侵，担心自己被诈骗。在谈话的过程中，我们说起"猜测"他人的密码到底有多简单。我告诉她很多人的所有账户都使用相同的密码，当她意识到自己就是这样做的时候，我发现她的面色有点发白。我又说起大多数人采用配偶的名字或生日以及纪念日来组合成简单的密码，她的面色转为苍白。我继续说到人们经常选择最简单的"安全问题"，例如"你（或你母亲）的闺名"，而这些信息通过因特网或者几个虚假电话就可以轻易获得。

很多人会将这些信息写在Blippy、Twitter或Facebook账户中。我这个朋友不常使用社交网站，所以我问她是否曾想到过，别人通过几个电话就可以得到这些信息，她当然说不可能。为了说明人们很容易提供个人信息，我告诉她自己曾经在一个餐馆看到一个餐具垫，上面说可提供当地高尔夫球场的50美元抵用券——真是个诱人的礼物。要拿到这个礼物，需要做的就是提供自己的姓名、生日和住址，同时提供一个密码，该密码将用来为你建立账户，该账号随后会发到你的邮箱。（我之所以很快注意到这个，是因为一些人已经在填写表格，并将表格放在了桌子上。）收集此类敏感信息的网站每天都会冒出不少。

一个问询电话或者简单的网络搜索就能够找到生日和纪念日信息。通过这些信息，可以建立

① 他的故事被好莱坞拍成电影*Catch Me If You Can*，译名《猫鼠游戏》或《逍遥法外》。——译者注

② 参见百度百科词条"维克多·拉斯体格"，网址是http://baike.baidu.com/view/3057089.htm。——译者注

口令攻击列表。而且，很多网站在出售各种个人信息，每人9美元到30美元不等。

了解恶意社会工程人员的思维方式、骗子对信息的反应以及诈骗犯诈骗的方式，人们能够对周边发生的事情更为警觉。

我和一些安全爱好者曾经遍搜互联网，找寻有关社会工程方方面面的故事。这些故事有助于回答一个重要的问题——“随着时间的推移，社会工程在现实中有哪些使用形式？”，从而发现社会工程在社会中的位置以及它的恶意应用方式。

## 1.2.1　社会工程及其定位

前面说起社会工程可以用于生活的很多方面，但是并非所有的应用都是带有恶意或者会带来伤害性结果的。很多时候，社会工程可以激励一个人采取对自身有益的行动。如何才能做到这一点？

考虑下面的情况。约翰需要减肥，他知道自己身体状况不太好，需要改善。约翰的所有朋友都处于超重状态，甚至觉得超重挺好，并且经常开玩笑说：“不用为体型操心，太棒了！”从另一方面来说，这是一种社会工程，体现为社会认可和共识，你可以通过身边好友的认可获得自我认可。因为约翰的好友都觉得超重没什么，所以他更易于接受这一点。不过，如果这些人中有一个减肥成功，并且没有因此而对其他人品头论足，相反却乐于帮助约翰，那么约翰对体重的看法可能会发生变化，开始认为减肥是可行的，而且还不错。

本质上来说，这就是社会工程。通过上面的例子，你可以清晰地看到社会工程在社会和日常生活中的应用。下面会列出几个社会工程、骗局和操纵的实例，并且分析其成功的原因。

### 1. 419骗局

419骗局又称尼日利亚骗局，已发展成为一种很流行的骗局。可以在www.social-engineer.org/wiki/archives/ConMen/ConMen-Scam-NigerianFee.html找到此骗局的故事和文章。

一般情况下，骗局开始于向目标发送一封邮件（近来是发送一条短信），告诉对方被选中进行一笔很赚钱的交易，但是需要他提供一个小小的帮助。如果目标愿意帮助发信人从一家外国银行提取一大笔钱，那么他也可以分到一部分。一旦目标相信了这件事，并且“愿意帮忙”，就会出现一个问题，而解决这个问题需要目标支付一定的费用。在付出费用之后，另外一个问题又会冒出来，需要支付另一笔费用。每个问题都是“最后一个问题”和“最后一笔费用”，但在几个月之后还会冒出新问题。整个过程中，目标不仅看不到一分钱，而且还会付出1万到5万美元。该骗局的惊人之处在于，过去报道过的骗局，有的采用官方文档、论文、书信抬头甚至面对面的欺骗方式。

最近，此类骗局出现了一种变化，受害者会收到一张真实的支票。诈骗者承诺一大笔钱，谎称自己仅要其中的一小部分。如果目标汇出一小笔钱（例如1万美元），当收到承诺的支票时，他

就可以兑现支票，留下其中的差额。有些案件中，受害者汇出了钱，但拿到的支票是假的，当他兑现支票时，会因兑现假支票而被处罚金。

这种骗局相当成功，因为它利用了受害者的贪婪心理。谁不想用1万美元换得100万，哪怕只是10万美元呢？大部分聪明人都会这样做。当这些人收到来自“政府职员”寄来的官方文档、护照、收据时，他们会信心十足地尽最大努力来完成交易。承诺、一致和义务等观念在其中发挥了一定的作用。我会在后续章节中对这些特征进行详细分析，到时你会看到此种骗局如此强大的原因。

### 2. 稀缺的力量

www.social-engineer.org/wiki/archives/Governments/Governments-FoodElectionWeapon.html上的文章讨论的是稀缺的原理。

当人们被告知，其需要或者想要的某样东西的供应量有限，且必须赞同某种观点或行为才能得到的时候，我们称这种情形为稀缺。很多时候根本不明确说明需要人们做什么，而是让他们看到行为“得当”的人得到了奖励。

文章中讲述的是南非利用食品赢得选举的例子。当一些人或某个人不支持“正确”的领导人时，粮食会变得稀缺，工作也会被那些支持者“抢去”。人们发现这个问题时，很快就会转变成支持者。这是一种恶意的、带有伤害性的社会工程，但是其思路值得学习。当人们发现某样物品短缺，并且相信某些行为会导致自己得不到该物品时，他们通常会愿意做任何别的事以得到它。上例里使情况更糟的是，政府拿走一些生活必需品，然后造成“短缺”假象，仅仅提供给支持者——这是一种恶意但很有效的操纵策略。

### 3. 员工窃贼

员工窃取公司信息的现象很普遍，www.social-engineer.org/wiki/archives/DisgruntledEmployees/DisgruntledEmployees-EmployeeTheft.html上发布的统计数据十分惊人，报告指出60%以上的受访员工承认从雇主处带走了各种各样的数据。

很多时候这些数据被卖给竞争对手（例如这个故事中摩根斯坦利员工的所作所为，详见www.social-engineer.org/wiki/archives/DisgruntledEmployees/DisgruntledEmployees-MorganStanley.html）；有时员工窃贼会掌握时间点或其他资源信息，在一些案件中，对公司不满的雇员会带来很大破坏。

有一次，我和客户讨论解雇员工的办法，谈到禁用门卡、关闭网络账户以及护送员工离开大楼等等措施。该公司则认为每个人都是“家庭”一员，这些办法并不合适。

不幸的是，在解雇吉姆的时候发生了问题。吉姆是公司的一个高层人员，解雇过程很顺利，吉姆很友好地表示理解。公司做对的一件事是在下班时间解雇他，这样会避免尴尬和干扰他人。

在握手之后，吉姆问了一个致命的问题："我可以再待一小时，清理桌子并从我的计算机中拷走一些个人照片吗？我会在离开的时候将门卡交给保安。"

由于对会谈结果很满意，他们很快就答应了，然后面带微笑地离开了。吉姆回到他的办公室，将所有个人物品放在一个箱子里，从计算机中复制了图片和其他一些数据，然后连接到网络，将11台服务器的重要数据清空（包括会计记录、工资单、发票、订单、历史数据及图片等），也就花了几分钟时间。吉姆按照约定归还了门卡，冷静地离开大楼，没有留下任何可以证明是他发起了这些攻击的证据。

第二天早晨，该客户打电话向我描述吉姆造成的破坏，期待找到解救的方法。他别无他法，只能尽可能取证恢复，并利用两个月之前的备份开始恢复系统。

一个未被检查的不满员工可能比一群虎视眈眈的专业黑客所造成的破坏还要大。据估计，仅仅在美国，由于员工窃贼导致的商业损失就高达150亿美元。

这些故事给我们提出了问题：社会工程人员到底有多少种？他们是否可以分类？

#### 4. 黑市和斯普林特大师

2009年，一则故事曝光了一个名为"黑市"的地下组织，"黑市"类似于罪犯的网络拍卖市场。该组织联系紧密，主要用于交易被盗的信用卡号、身份盗用工具及身份伪造工具等物品。

穆拉斯基（J. Keith Mularski）是美国联邦调查局的一名探员，他秘密打入了这个地下组织。一段时间以后，穆拉斯基探员成为了该网站的管理员。尽管该组织有很多人对他心存怀疑，但他还是管理这个网站长达3年之久。

在这段时间里，穆拉斯基必须伪装成恶意黑客，说话、行动与思考的方式必须一致。他伪装成一名恶意垃圾邮件发送者，这方面丰富的知识也是他成功渗透的基础。他的伪装和社会工程技巧之所以大获成功，是因为他使用了不起眼的斯普林特大师（Master Splynter）的身份进入了黑市网站，3年之后整个身份盗用团伙被摧毁了。

3年的社会工程渗透行动让59名罪犯落入法网，阻止了7000多万美元的银行欺诈。这仅是社会工程技巧具有积极作用的一个范例。

### 1.2.2　社会工程人员的类型

前面说到社会工程有很多不同形式，既可以是恶意的，也可以是善意的，既可以具有激励作用，也可以具有毁灭性。在学习本书的核心内容之前，我们首先简单介绍一下各种形式的社会工程人员。

- **黑客** 软件厂商生产的软件的安全性能不断提高，攻击软件因此变得越来越难。由于对于软件和网络的攻击（例如远程入侵）越来越困难，现在黑客开始采用社会工程攻击方式。目前在世界各地，通过利用硬件技术和一些个人技巧，黑客在大大小小的攻击中都会使用社会工程。
- **渗透测试者** 因为现实世界的渗透测试者（也称做渗透者）本质上有很强的攻击性，所以此类人员仅次于黑客。真正的渗透测试人员会学习和使用恶意黑客所使用的技巧，帮助确保客户的安全。他们拥有恶意黑客的技巧，但不会利用攻击中所取得的信息获利，也不会伤害目标。
- **间谍** 间谍把社会工程当成一种生活方式，他们通常会利用社会工程框架（本章稍后会讨论）的每一方面，可以说是这门学科的专家。世界各地的间谍都会学习"愚弄"人的方法，能够让人相信他就是某人或不是某人。除了学习社会工程技巧之外，间谍还或多或少地了解所渗透的企业或政府，这样才能得到他们的信任。
- **身份窃贼** 身份窃贼在当事人不知情的情况下，使用他人的名字、银行账号、地址、生日和社会安全号码等个人信息。这种犯罪的形式多样，包括穿上某种工作服来冒充该行业的人，也包括设置精巧的骗局。身份窃贼也会利用各种社会工程技巧，随着时间的推移，他们会变得更加大胆，对他人的损失更加漠不关心。
- **不满的员工** 在员工对公司感到不满之后，他们和雇主的关系常会进入敌对状态。这经常是单方面的情形，因为员工会故意隐藏不满的程度以降低职业风险。但当不满加剧时，他们就可能进行盗窃及破坏等各种犯罪了。
- **高明的骗子** 骗子总是利用他人的贪婪等心理，诱发人们"发财致富"的想法。高明的骗子会读心术，通过一些小细节就能确定某人是不是合适的"目标"。他们在造势方面也相当有技巧，让目标认为这是天赐良机。
- **高端猎头** 猎头也必须懂得社会工程的技巧，包括诱导和社会工程的心理原则。他们是读懂人们心理和动机的高手。很多时候，猎头不仅需要考虑和迎合求职者的需求，也要全面审视雇主的想法。
- **销售人员** 与猎头类似，销售人员也必须掌握很多人际交往的技能。很多经验丰富的销售人员都说，一名出色的销售人员不需要操纵他人，而应该利用自己的技巧发现人们的需求，并且看看自己是否能满足这些需求。销售的艺术包括信息收集、诱导、影响、心理把握以及很多人际交往的技能。
- **政府** 虽然政府很少被视为社会工程人员，但是政府会利用社会工程来控制信息的发布并管理人民。很多政府部门利用社会认同、权威性和稀缺资源来确保目标的受控性。这类社会工程并不总是负面的，因为一些政府传递的信息是对人民有利的，而且通过利用一些社会工程因素，这些信息会更有号召力，也更容易被广泛接受。
- **医生、心理医生和律师** 从事这些职业的人员似乎与其他社会工程人员不一样，但是他们同样使用上述社会工程人员所采用的方法。他们必须采用诱导、正确的谈话方式和询问策略，以及社会工程的许多（乃至全部）心理原则，来操纵"目标"（客户）采取他们所期望的行动。

不管在哪个领域，你都可以发现社会工程或其某一方面的应用。这也是我坚信社会工程是一门科学的原因。社会工程的各要素相加等于达成的目标。以骗子为例，伪装+操纵+贪婪心理=目标被社会工程套牢。

每一种情况下，困难都在于知道哪些要素会起作用，但是学习每个要素的使用方法就需要技巧了。这是制定社会工程框架的理念基础。正如下一节将讨论的，社会工程框架彻底改变了人们分析社会工程的方式。

### 1.2.3　社会工程的框架及其使用方法

我根据个人的经验和研究列出了社会工程人员需具备的各个要素。这些要素都很重要，具备所有要素才能成为一名合格的社会工程人员。这些要素并非一成不变。事实上，从建立开始，框架已经有了很大的发展。

这个框架的目的在于为学习这些技巧的人提供足够的信息，它并非每章包含的所有信息的资源参考。例如，第5章中有一部分是关于微表情的，内容源于该领域一些杰出人士的研究和我使用这些信息的经验。这些内容绝不可能替代保罗·艾克曼（Paul Ekman）博士等杰出人士在该领域50年的研究成果。

在通读框架之后，你会发现利用框架中的很多技巧不仅可以提高安全实践水平，而且也可以提高自身安全防护、有效沟通和理解他人的能力。

参考本书目录可大致了解框架，也可以在www.social-engineer.org/framework上查看该框架。框架乍看上去有点难以理解，但本书中对各个课题都进行了分析，你将学会如何应用每个技巧，并不断增强技能。

知识就是力量——诚哉斯言。掌握知识是防御大部分社会工程攻击的最佳手段。即使知识不能提供百分之百的防护，详细了解攻击手法也会让你保持警惕。学习知识不仅可以增强自身技能，而且还可以让你提高警觉。

除了学习，还要动手练习。本书并非仅需阅读一次的手册，而是一本学习指南。你可以根据需要对每节的课题进行学习和练习。框架内容是循序渐进的，因为社会工程攻击也是如此。框架按照社会工程人员在实践中或计划阶段利用技巧的顺序来讨论各个技巧。

框架展现了攻击的要点。在攻击计划完成之后、交付之前，必须要研究、增强和练习相关的技巧。

假设你需要为一家公司策划一次社会工程审计，目的是看你是否能够进入其服务器机房获得其中的数据。

也许攻击计划是伪装成需要进入服务器机房的技术支持人员。那你就需要收集信息，甚至需

要进行垃圾搜寻。

由于需要伪装成技术人员，你可以采用隐秘的摄像工具捕捉相关信息，练习技术人员的语言、脸部表情/声音，让你在行动、声音及表情上看起来就是一名技术人员。

如果能找到为客户提供技术支持的公司的名称，也需要收集他们的信息。你的客户通常要谁来提供服务呢？具体联系人的姓名是什么？攻击需要适当地计划。

不过本书并非仅为执行审计工作的人员所写。很多读者想知道攻击是什么，不是为了保护公司，而是为了保护自身。不清楚恶意社会工程人员的思维方式，其结果就是很容易被攻击。

大学中主修安全的学生也在使用这个框架。框架中列出了这些攻击的实现方法，读者可以深入学习。

一般来说，这些信息也可以提高每个人的日常沟通能力。通晓怎样读取面部表情或怎样提问会让他人更加放松并引出正面的回应，可以提高你与家人和朋友沟通的能力。它会帮助你成为一个好的倾听者，让你更加关注他人的感受。

读懂身体语言、面部表情和语调信息也可以增强你的沟通能力。知道怎样保护自己和你爱的人，会提升你的价值，让你对外部世界更加敏感。

## 1.3　小结

和其他任何书籍一样，只有付诸实践，书中知识的价值才会得以体现。实践得越多，对这些技能的掌握也就越成功。

前面我说过社会工程和烹调十分相似。通过将各种正确的调料进行适量混和，可做成令人垂涎欲滴的美味佳肴。第一次尝试烹调时，菜可能做得过咸也可能淡而无味，但是你不会轻易放弃，通过不断尝试，终会得偿所愿。社会工程也一样。一些必须掌握的技巧可能轻而易举就学会了，而有些技巧则难学得多。

如果某个课题很难理解或很难掌握，请不要放弃，也不要认为自己学不会。只要付出努力，任何人都能学会和使用这些技巧。

同时也要记住，与烹饪秘方一样，成功的社会工程也需要很多“配料”。第一种配料可能在一段时间后才会发挥作用。有些技巧，例如第5章介绍的“人类思维缓冲区溢出”，只有在你掌握书中的一些其他技巧之后才有意义。

不管怎样，要反复练习，对没搞清楚的课题要进行额外的研究。现在，让我们开始“烹调”吧。你的“秘方”起始于下一章的第一味配料——信息收集。

# 第 2 章 信息收集

战争的胜利百分之九十取决于情报。

——拿破仑·波拿巴

人们常说，没有什么信息是不相关的。本章的主题是信息收集，这句话放在这里完全适用。即使是最微小的细节也可能促成社会工程人员的成功入侵。

我的良师益友马蒂·阿哈罗尼在渗透测试方面有十多年的专业经验，他的一次亲身经历是这方面最好的例证。那次，马蒂的任务是入侵一家在网上查不到什么信息的公司，因为能入侵该公司的途径很少，所以这项任务极具挑战性。

马蒂开始通过互联网寻找可能取得突破的任何蛛丝马迹。一次搜索中，他发现该公司一名高管的公司电子邮件地址出现在了一个集邮论坛上，且该高管对20世纪50年代的邮票表现出了浓厚的兴趣。马蒂迅速注册了一个域名，类似于www.stampcollection.com，然后从谷歌上找来一堆20世纪50年代的邮票图片。他快速创建了一个网站展示他的“集邮册”，随后又精心编写了一封电子邮件发给该高管。邮件内容如下。

亲爱的先生，

我在www.forum.com上发现你对20世纪50年代的邮票很感兴趣。最近我的祖父过世了，给我留下一个集邮册，我想出售这批邮票。我建了一个网站，如果你想看的话，请访问www.stampcollection.com。

谢谢！

马蒂

在给目标发送电子邮件前，他想确保产生最大的影响。他找出论坛帖子中该官员办公室的电话号码，给他打了个电话，说："早上好，先生，我是鲍勃。我看见你在www.forum.com上发的帖子。 我爷爷最近过世了，给我留下了一大堆20世纪五六十年代的邮票。我拍了照片，并且做了一个网站。如果感兴趣的话，我可以将链接发给你看看。"

目标非常急切地想看到这些邮票，就等着收电子邮件了。马蒂发送完电子邮件后，便等待他点击链接。马蒂将一个恶意帧嵌入到网站页面中，帧中的代码会利用当时很流行的IE浏览器的已知漏洞，使目标计算机受控于马蒂。

不久，受害人就收到了邮件，而且迫不及待地点击了链接，公司系统的边界防御也就打开了。

短短的一条信息（受害人寻找邮票时留下的公司邮箱地址）就导致了这次入侵的发生。所以我们说，没有信息是不相干的。带着这样的思想，我们来看看信息收集中会碰到的问题。

- 怎样收集信息？
- 社会工程人员收集信息可以利用的资源有哪些？
- 如何利用收集到的信息进一步描述目标？
- 如何对这些信息进行定位、存储及分类，才能够使之最易于使用？

为了完成适当而有效的信息收集工作，这些只是需要解决的问题中的一小部分。在多如牛毛的社交网站上，人们可以轻易地与其所选的人分享自己生活的方方面面，这使潜在的破坏性信息比以往任何时候都多。本章通过社会工程实例讲解信息收集的原则和应用，以及人们发布在网上的信息对于其个人和企业安全有何破坏性的影响。

社会工程人员使用到的很多技巧或方法都来自于其他领域，其中一个典型的例子就是销售。销售人员往往很健谈、随和，而且非常善于收集别人的信息。

我曾经读过一本有关销售的书，作者鼓励销售人员去收集购买者的推荐，其中有个问题是这样的："你认为谁能像你一样从该产品中受益呢？只要说一个人就可以。"

只需要简单的交流就可以让一个人敞开心扉，他可能推荐家人、朋友甚至同事。收集这些信息使销售人员可以在"熟人介绍"的情况下拜访客户，并能够迅速获得对方的信任，不至于吃闭门羹。

销售人员在拜访时可以使用如下开场白："我刚从隔壁的简家里过来，她买了我们的优惠套餐。在了解各种好处之后，她支付了一年的套餐费用，并认为你也能从中受益。请问能耽误你一分钟，听我介绍一下简刚刚买的优惠套餐吗？"

销售人员使用的这些技巧经常被社会工程人员效仿。当然，社会工程人员并不会要求交谈的对象推荐他人，而是自己通过分析得到其中的信息。销售人员从当前客户处收集信息，然后利用这些信息使新的"目标"客户更乐于倾听并接纳自己的建议。此外，通过暗示前一位顾客已购买，

并在交流中使用“优惠”、“优先”等关键词，销售人员在短时间内就使目标兴趣盎然。这种技巧很有效，因为它建立了信任，利用了“熟人”，能让目标跨越最初的沟通障碍，与销售人员或社会工程人员更为自然、舒服地交流。本章以及第3章将深入探讨这些话题。

作为社会工程人员，这两个角度对于理解和有效运用技巧都至关重要。回想一下第1章中对主厨的相关阐述：一位优秀的主厨知道如何辨认出高质量的菜肴、新鲜的蔬菜和优质的肉类。他们很清楚秘方中的配料，但若不能把握好各食材的用量，这道菜要么淡而无味，要么偏咸，甚至会难以下咽。想要成为主厨，仅仅知道菜里需要放盐是远远不够的，还需要了解适量的各种配料如何搭配，这样才能掌握烹饪的艺术。社会工程人员只有牢牢掌握各种技术手段的使用方法和适用场景（“秘方”），才能成为社会工程达人。

本章帮助你找到平衡点。信息便是社会工程人员“秘方”里的首要配料，下一节会详细介绍。信息质量越高，成功的几率就越高。本章从如何收集信息讲起，然后讨论通过哪些途径来收获信息，最后将讨论如何整合各类信息并运用到社会工程中，这样本章在体系上就很完整了。

## 2.1　收集信息

收集信息就如同盖房子一般。如果想从房顶盖起，肯定是必败无疑。一栋坚固的房子必定是在打下坚实的地基后，从地面往上盖的。收集信息时不要总想着怎么组织和运用这些数据，创建一个文件或信息收集服务来收集信息才是当务之急。

事实上，有很多工具可以帮助我们收集和运用这些数据。在渗透测试和社会工程审计中，我使用Linux BackTrack发行版，BackTrack是专为这一目的而设计的。BackTrack[1]和大部分Linux发行版一样，是免费、开源的，也许它最大的优点便是集成了300多款安全审计工具。

BackTrack中的工具也是开源和免费的。特别吸引人的一点在于这些工具的质量都很高，其中很多都能与同类商业软件媲美，甚至是有所超越。这其中就有两个特别适用于信息收集和存储的工具，一个是Dradis，另一个为BasKet。接下来将分别简要介绍这两款工具。

### 2.1.1　使用BasKet

BasKet从功能上看有点像记事本，但是比记事本要强大得多。这款软件现在由王凯文（Kelvie Wong）维护更新，你可以从BackTrack中找到，或者到http://basket.kde.org/网站上免费下载。该网站有详细的介绍，教你如何安装。这款软件易于使用，界面也并不复杂。

① BackTrack是基于Ubuntu的自启动运行光盘，它包含了一套安全及计算机取证工具，简称BT，目前最新与最好用的版本是BT5。——译者注

如图2-1所示，界面很简单，很容易上手。在屏幕左侧单击鼠标右键，选择“New BasKet”，会添加一个新的“BasKet”，用以保存数据。

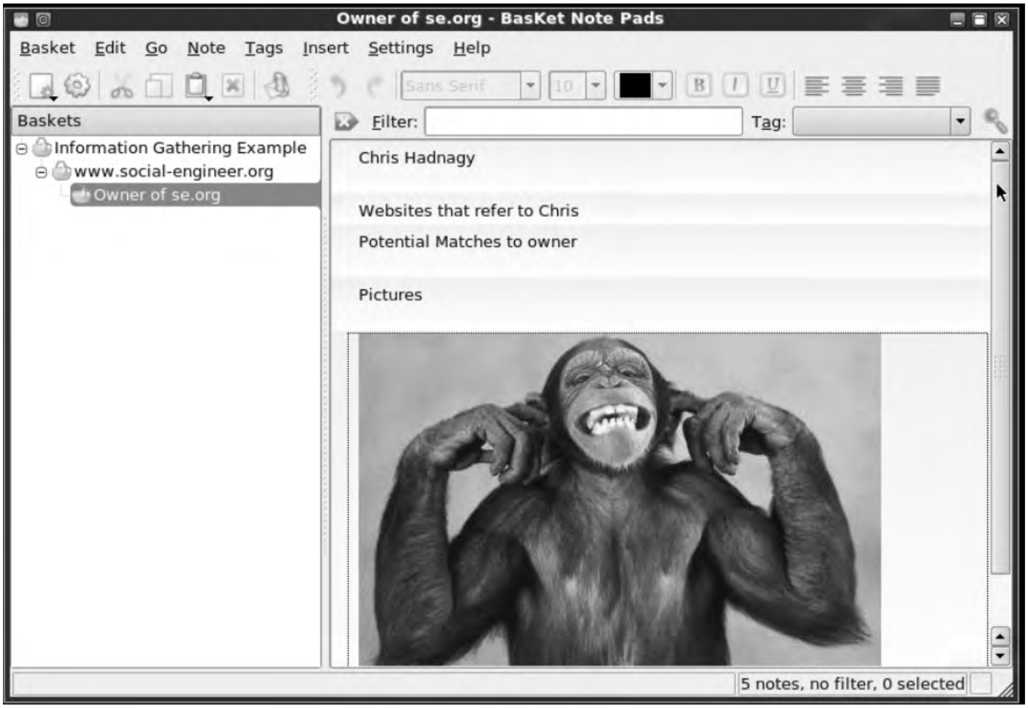



图2-1　信息收集阶段，使用BasKet轻松组织收集到的数据

BasKet新建好以后，便可以往里面复制/粘贴数据，添加屏幕截图，甚至可以添加OpenOffice办公软件或者其他类型的图表数据。

添加屏幕截图的方式有好几种，最简便的方法是复制图片，在新“BasKet”中单击鼠标右键，选择“粘贴”。如图2-1所示，添加图片的操作简单、快捷，同时可以通过输入、粘贴等各种方式为图片添加文字备注。

在通常的安全审计中，BasKet组织和展示数据的方式是它的优势之一。我通常为不同类型的数据建立不同的BasKet，例如域名查询信息、社交媒体信息等。然后，使用谷歌地图或谷歌地球获取目标客户的建筑和设施图片，保存到BasKet中。信息收集完成后，快速提取和使用这些信息也很简单。图2-2展示了一个接近完工的BasKet，其中有很多有用的信息和标签。

如图2-2所示，使用BasKet来存储和组织信息很简单。我尽可能多地往里面存放信息，因为再小的信息也可能是有用的。我收集的信息包括目标客户的网站内容、域名查询信息、社交网络、图片、员工联系方式、简历、论坛、爱好等一切可能与目标公司相关的信息。




图2-2　包括很多有价值信息的几近完整的BasKet截图

信息收集完成之后，直接单击“BasKet”菜单，然后单击“Export”，将整个BasKet导出为HTML网页文件。这对生成报告和共享信息非常有用。

对于一名社会工程人员来说，接下来要详细讨论的数据收集是每次行动的核心。然而，如果信息不能得到及时的重现和运用，将会毫无价值。BasKet及其类似工具使得信息收集和使用工作更加简单。一旦你尝试使用，便会爱不释手。

## 2.1.2　使用Dradis

尽管BasKet是款非常好用的工具，但是如果要收集的信息很多，或者需要一组人共同完成信息收集、存储和调用操作，那么就需要一款能够供多用户共享数据的工具——Dradis。根据Dradis工具开发者的描述，Dradis是可以提供信息中央存储的独立Web应用，可以统一管理需要收集的信息。

和BasKet一样，Dradis也是一款免费的开源工具，你可以在http://dradisframework.org/网站上免费下载。Dradis可以安装于Linux、Windows和Mac等不同操作系统，http://dradisframework.org/install.html网页上有详细的安装和配置说明。

Dradis安装并设置好以后，就可以浏览你分配的本地主机和端口，或者使用标准端口号3004。只要打开浏览器，在地址栏中输入http://localhost:3004/即可登录使用。

登录进去以后的欢迎界面如图2-3所示。注意左上角的添加分支（Add Branch）按钮，添加分支以后就可以像BasKet一样添加信息，如备注、图片等，甚至可以导入笔记数据。

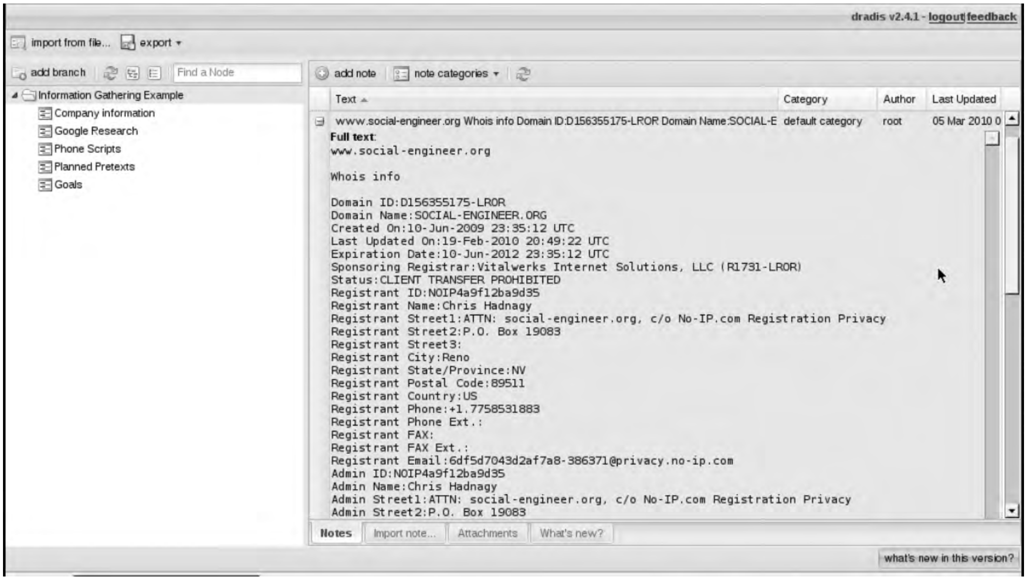



图2-3　Dradis简洁而易用的界面

Dradis和BasKet只是用来收集和存储数据的两款小工具，二者的网站上都有很好的设置说明和使用介绍。

不论操作系统是Mac、Windows还是Linux，你都能找到相对应的工具。重要的是工具用起来顺手，并能处理大规模数据。

基于上面提到的因素，我建议社会工程人员放弃使用Windows或Mac操作系统自带的记事本和文本编辑器。它们无法满足你对于数据格式和相关区域高亮显示的需求。图2-3显示的是我使用的Dradis服务器端，有一部分我专门用来保存电话交谈记录。这个功能很好用，可以记录我根据所收集的信息产生的想法。

这些工具表明了社会工程人员是怎样利用收集到的信息的。利用信息的第一步便是要像社会工程人员一样思考。

### 2.1.3　像社会工程人员一样思考

拥有几百兆的图片和数据固然很好，但是当你回过头来浏览这些信息时，如何能够保证最大限度地挑出有用的信息呢？

当然，你可以打开浏览器，随机输入冗长的词语进行关键词搜索，这样做可以找到某种形式

的信息，其中一些甚至是有用的。然而，在肚子很饿的情况下，你才不会跑到厨房，不管三七二十一地往锅里随便扔食材，然后就开始翻炒呢。计划、准备并考虑各种会影响菜肴好坏的因素才可能烹饪出佳肴。同理，社会工程人员也要做好计划和安排，想好将要收集的信息和收集的方式才可能成功。

信息收集的关键一步是要转换自己的思维方式。在信息大爆炸的世界，我们必须改变平常的思维方式，学会质疑一切，看到信息时就按照社会工程人员的思维方式来思考。利用网络等方式进行搜索的方式要改变，对于网页上返回的信息，也要学会从社会工程的角度去思考、审视。无意中听到的谈话、论坛上看似无聊的帖子，抑或是一袋垃圾，都应该以不同的方式来对待。我的导师马蒂看到程序崩溃就异常兴奋。为什么？他是渗透测试员，同时也是漏洞编写人员，崩溃是找到软件漏洞的第一步。因此，当遇到程序崩溃时，他感到异常兴奋，而不是为数据丢失而烦躁焦虑。作为社会工程人员，也必须要对信息抱有同样的态度。每当发现目标人物使用多个社交网站时，便将它们之间的联系和信息数据收集起来综合分析，争取得到完整的目标人员档案。

举个例子来说，有一次我要去遥远的另一个州办事，便租了一辆车。我和同事将行李统统装到了后备箱。我们刚要上车，就发现后座上有一小袋垃圾。同事说："如今的服务真差，我们付钱租车，他们至少应该将车子打扫干净吧。"

诚然，大家都希望车子里是干干净净的，同伴想把它扔到旁边的垃圾桶里，我阻止了他，说道："让我看看那个袋子。"我打开袋子，拨开里面的快餐纸袋以后，映入眼帘的物品让我大吃一惊——里面是半张撕碎的支票。我赶紧倒空袋子，从里面找到一张银行收据还有另外半张支票。这是一张面值几千美元的支票，虽然被撕开了，但撕得不是很碎，仅撕成了四大块，然后被扔到装有快餐纸袋的垃圾袋中。将这几片拼接到一起，可以看到这张支票的所有者的姓名、公司名称、地址、电话号码、银行账号及银行流水单号。再加上这张银行收据，我可以清楚地知道他的存款数字。他应该感到庆幸，我不是心存歹念的人，要不然只要再多几步，我就可以从他的账号中窃取存款。

这个故事向我们展示了人们是如何看待自己的重要信息的。这个家伙在我之前租了这辆车，他可能以为将支票撕碎扔掉就安全了，或者说至少当时他是这样认为的。无独有偶，通过www.social-engineer.org/wiki/archives/BlogPosts/LookWhatIFound.html，你可以看到最近发生的这样的故事：有人将非常贵重的物品随意扔掉，或者在旧货市场上廉价出售。

其中包括：

- 一幅被博物馆以120万美元收购的油画；
- 一辆1937年生产的、仅跑了24 000英里的型号为57S Atalante的布加迪跑车[①]，这辆车最终以300万美元出售；

① 布加迪公司在过去70多年时间里仅生产了3辆Atalante原型车，其中只有2辆存世至今，而57S型Atalante轿车在后来的限量生产试验中也仅生产了17辆。目前为止有4辆被保存在法国乡村的博物馆里，该车留存数量极少，找到的这辆57S Atalante布加迪跑车已经消失了半个世纪之久。——译者注

- 《独立宣言》珍本。

如果人们能把《独立宣言》珍本随同一张油画扔掉，那么丢掉账单、医疗记录、旧发票或者信用卡账单又有什么大不了的。

懂得如何在公共场所和人打交道会产生令人意想不到的效果。接下来将讲述我对一家公司进行安全审计的经历。在审计之前，需要收集一些数据。下面就让我们看看，如何利用那些看似无用的信息找到突破口。

对于被审计公司的一位高管，我仅仅跟踪其一两天，便发现了他每天早上同一时间都会去当地一家咖啡馆喝咖啡。在发现他的这一习惯后，我便计划了一场“偶遇”。他一般早上7:30到咖啡店，每次会坐半小时到35分钟的样子，看看报纸，喝一杯中杯拿铁。在他进店3~5分钟后，我也进到店里，点了相同的咖啡，坐到他旁边的位子上。我看到他放在一旁已经看完的报纸，便向他借阅。路上我已经读过了这份报纸，知道第3页上有一篇关于附近一起谋杀案的报道。我装作刚看到这则消息一样，大声说道：“在这么小的一个镇子里，怎么会有如此骇人的事情发生，太可怕了！你是不是也住在这附近啊？”

此时此刻，有两种可能：一是他根本不理我，二是我的肢体语言、说话的语调和表现会让他感到放松。事态的发展证明是第二种情况，我成功了。他答道：“是啊，几年前我因为工作搬到这里。我喜欢小城镇，但正如你所说，这种可怕的事情越来越多。”

我接着说道：“我只是途经这里。我的工作是给大公司提供高品质的咨询服务，我经常在不同的小城镇之间跑来跑去。不过最近这种事情越来越多了，就连乡下也是如此。”之后，我用一种调侃的语气问道：“你不会碰巧是一个需要咨询服务的大公司的领导吧？”

他笑了起来，感觉我刚刚的话是在质疑他的高贵身份一般，说道：“我是XYZ公司的财务副总，不过我不负责那个部门。”

“嘿，我又不是在向你推销产品，喝咖啡而已。不过，不知你明天或者周三有没有空？我可以顺便访问贵公司并为你提供一些信息。”

从这里开始，故事变得有趣了。他说：“我很想应约，但是周三我必须要出去度假。要不你给我发份邮件，我回头给你电话。”并随手递上了他的名片。

“我猜想应该是去和煦而明媚的地方吧？”我问道，心想快达到目的了，是时候结束此次谈话了。

“和我妻子一起乘游艇去南方。”我想他是不会告诉我目的地的，不过这也没关系。我们握了握手，便分道扬镳了。

他会很快忘记我吗？也许吧。不过，我已经得到一些颇有价值的信息了：

- 他的直拨电话号码
- 他出发去度假的日期
- 度假的类型
- 他住在本地
- 他公司的名称
- 他在公司的头衔
- 他是近期搬过来的

当然，其中一些信息在我前期信息收集时就知道了，但是这次会面让我得到了更多信息。现在可以开始我的下一步攻击了，在他去度假的翌日，我拨通了他公司的直线电话，前台告诉我：“对不起，史密斯先生度假去了，请问需要留言吗？”

太好了。信息的真实性已被证实，我要开始计划的最后一步了。我穿上西装，带着价值9美元的名片来到他的公司。进去登记好之后，我告诉前台自己和史密斯先生约定10点钟会面。她答道：“史密斯先生在度假，你确定是今天吗？”

使用我的微表情技术（第5章会讨论到），我故作惊讶地问道：“什么？他的海上航游是在这周？我以为他下周才出发。”

刚刚的这句相当关键。为什么？

我想让前台相信我，相信这个会面是真实的。在我提到海上航游时，说明我和史密斯先生有过亲密的交谈，甚至于知道他的旅行计划。我流露出的无助和失落引发秘书想帮助我的冲动：“哦，亲爱的，真的很抱歉，要不我给他的助手打个电话吧？”

“哦，不。”我答道，“我只是想给他带来一些信息。这样吧，我把消息给你，在他回来时，你帮忙转告他。真的是太尴尬了，你可以不告诉他我来过吗？”

“我会保守秘密的。”

“谢谢你。真想快点离开这里，不过在我离开之前，可以用一下这里的洗手间吗？”通常情况下这种要求应该是不被允许的，但是借着刚才融洽的对话、我的无助以及她对我的一点同情，我还是有一些机会的——而且我确实成功了。

我把一个信封放在了洗手间的一个隔间里。信封上贴着“私人”的标签，信封里面是一个带有恶意攻击病毒的U盘。不仅是这里，我在大厅走廊旁的休息间里也放了一个，以增加成功的概率。希望有人会发现当中的一个，并好奇地将U盘插到他们的电脑里。

值得庆幸的是，这种方法百试不爽。可怕的是，如果没有那次咖啡店里看似无足轻重的对话，这次攻击不可能成功。

这个故事不仅是要说明微小的数据也会导致入侵事件，同时也展示了搜集数据的技巧。对待各种数据源必须充分理解、认真测试，直到你能熟练掌握每一种数据源及其收集方法。数据源有很多种，优秀的社会工程人员必须花费一定的时间来了解每一种的优缺点，以及利用它们的最佳方法。这也是下一节要讨论的内容。

## 2.2 信息源

信息存在多种不同的来源。虽然以下几个小节不能覆盖每一种来源，但是也列出了收集信息的主要途径。

### 2.2.1 从网站上收集信息

公司或者个人网站是信息的重要来源。优秀社会工程人员的第一步就是尽可能多地从公司或者个人网站上收集信息。在这些网站上花费一些时间是值得的，可以帮助你清晰地了解对象的基本情况：

- 他们做什么
- 他们提供的产品和服务
- 地理位置
- 招聘信息
- 联系电话
- 执行官和董事会成员的简介
- 支持论坛
- 电子邮件命名规则
- 可能用于密码分析的特殊字符或短语

看别人的个人网站是件非常有意思的事情，因为上面的内容涉及他们生活的方方面面：孩子、房子、工作等。这些信息应该分类存储，因为它们常会用于日后的攻击。

同一个企业的员工往往会登录相同的论坛，有着类似的兴趣，甚至会上相同的几个社交网站。如果你在LinkedIn或者Facebook中找到一名员工，很有可能他的好几个同事也在其中。收集这些数据，可以更加清楚地分析这家公司以及它的员工。很多员工会在社交网站上用标签的形式展示自己的职位，这可以令社会工程人员勾勒出公司某个部门的规模以及组织架构。

#### 1. 搜索引擎

强尼·龙（Johnny Long）为渗透测试人员写了本著作，叫做*Google Hacking for Penetration Testers*。这本书让很多人大开眼界——原来谷歌里有如此多的信息。

谷歌中记录了很多你认为已经删除的数据，就如同大型数据库一般。只要设定好查询方式，就能得到你想要的信息。

强尼总结出了一系列用来查询公司信息的语法。例如，在谷歌搜索框中输入site: microsoft.com filetype:pdf，就能得到microsoft.com网站上的所有PDF文档列表。

熟知搜索语法可以帮助你找到和目标相关的信息，这对信息收集来说很重要。我习惯于使用语法（类似于filetype:pdf）来检索PDF、DOC、XLS和TXT文件。当然，员工留在服务器上的DAT和CFG文件以及其他数据库和配置文件等也是值得收集的信息。

强尼的书通篇都在讨论如何利用谷歌来查找数据，不过重点是懂得谷歌提供的各种操作符可以帮助你创造出属于自己的搜索语法。

www.googleguide.com/advanced_operators.html上列出了各种操作符以及详细使用方法。

能够提供惊人信息量的搜索引擎不止谷歌一家。一位名叫约翰·玛瑟利（John Matherly）的研究人员发明了一个叫做“Shodan”的搜索引擎（www.shodanhq.com）。

Shodan的特殊之处在于它提供针对服务器、路由器和特定软件的搜索功能。例如搜索microsoft-iis os:“windows 2003”，就可以得到如下各地的服务器数量信息，这些服务器都是运行IIS服务的，里面装的是微软Windows 2003系统。

- 美国 59 140
- 中国 5361
- 加拿大 4424
- 英国 3406
- 台湾 3027

这个搜索引擎不能针对特定目标，但是它揭示了一个道理：网络上有惊人的信息量供社会工程人员查询分析，以提升信息收集的能力。

#### 2. Whois域名信息查询

Whois能提供域名数据库查询服务。Whois数据库中有很多有价值的信息，有些时候甚至包括网站管理员的完整联系方式。

使用Linux命令行工具或者登录www.whois.net这样的网站，都可以查询到域名的注册信息，包括联系人、电子邮件地址、电话号码，甚至DNS服务器的IP地址。

域名注册信息可以很好地帮助你了解目标公司，特别是他们的服务器。这些都可以用于信息的进一步收集，或者发动攻击。

### 3. 公共服务器

企业对外的公共服务器往往会提供网站所没有的很多信息，比如服务器的操作系统、安装的应用程序和IP地址，这些信息可以大致反映企业的信息服务架构。了解平台和应用信息之后，便可以和域名信息组合在一起，在公开技术论坛上进一步搜索相关的配置信息。

IP地址可以说明服务器是在本地还是从服务器提供商处租赁的；通过域名解析记录可以看出服务器的名称、功能，以及IP地址分布。

在一次审计的过程中，通过使用Matelgo（第7章中将有详细介绍）搜索网页，我找到了一个对外的网站服务器，上面有几百份文档，其中包含项目数据、客户和文档作者信息。这些信息的泄露，对于公司来说是致命的。

值得一提的是，*端口扫描*（使用诸如NMAP或者其他端口扫描工具去定位公共服务器的开放端口、软件版本和操作系统类型等）在有些地区是违法的。

2003年6月，以色列人艾维·米兹拉希（Avi Mizrahi）因涉嫌未授权访问计算机系统被当地警方提起公诉。当时，他只是对摩萨德网站（Mossad）进行了端口扫描。8个月后，艾维被无罪释放。法官的意见是非恶意的端口扫描不应被禁止（www.law.co.il/media/computer-law/mizrachi_en.pdf）。

1999年12月，斯考特·莫尔顿（Scott Moulton）被联邦调查局以违背佐治亚州《计算机系统防护法》和美国《计算机欺诈与滥用法》为由实施逮捕。当时，他所在的IT服务公司与佐治亚州的切罗基县有着长期的合作关系，一直为911安全中心提供维护和升级的服务（www.securityfocus.com/news/126）。

作为工作的一部分，莫尔顿在为切罗基县的服务器进行例行端口扫描时，扫描到另外一台属于另一家IT公司的网站服务器。这件事情直接导致其被起诉，到了2000年，法官以未对互联网完整性和可用性造成破坏为由，撤销了对他的诉讼。

2007年到2008年间，英国、法国和德国都通过了相关的法律，认为创建、发布和拥有能够导致他人入侵计算机的工具都是违法行为，端口扫描工具也在其中。

当然，如果是收费的信息安全审计，这些都应在合同中描述清楚。对社会工程人员来说，应该熟知当地法律，避免做出违法行为，这非常重要。

### 4. 社交媒体

很多公司最近开始热衷于在社交网站上做推广和营销。社交网站的营销成本低廉，又有大量的潜在消费群体。这里提供了来自于企业的另外一股信息流：活动安排、新产品发布、新闻报道以及一些能与当前热点事件挂上钩的文章，等等。

近期，社交网络正在逐步显示它们的作用。每当一个站点成名，便会涌现一系列采用类似技

术的站点。有了Twitter、Blippy、PleaseRobMe、ICanStalkU、Facebook、LinkedIn、MySpace等站点以后，人们的生活和行踪被晒在了网上。随后，我们将深入讨论这一话题，你将发现社交网络作为信息源的神奇之处。

#### 5. 个人网站、博客等

像博客、维基、网络视频等个人网站不仅会提供目标公司的信息，还会透漏这些信息上传者的个人观点和信息。在博客上对企业满腹牢骚的员工会和那些持有类似观点的人相聊甚欢。不管以什么样的方式，人们总会在网上张贴大量的数据信息，任何人都可以阅读。

举个例子。让我们一起来看看最近出现的一个网站——www.icanstalku.com（参见图2-4）。不同于它的域名，这个网站并不是鼓励人们去跟踪别人，它跟踪的是那些毫无防范意识的Twitter用户。它遍历Twitter网站，寻找那些蠢到用自己的智能手机拍摄照片并上传的家伙。很多人都没意识到智能手机拍摄的照片会隐藏GPS信息。你上传这些照片的同时，也泄露了自己的拍摄位置信息。

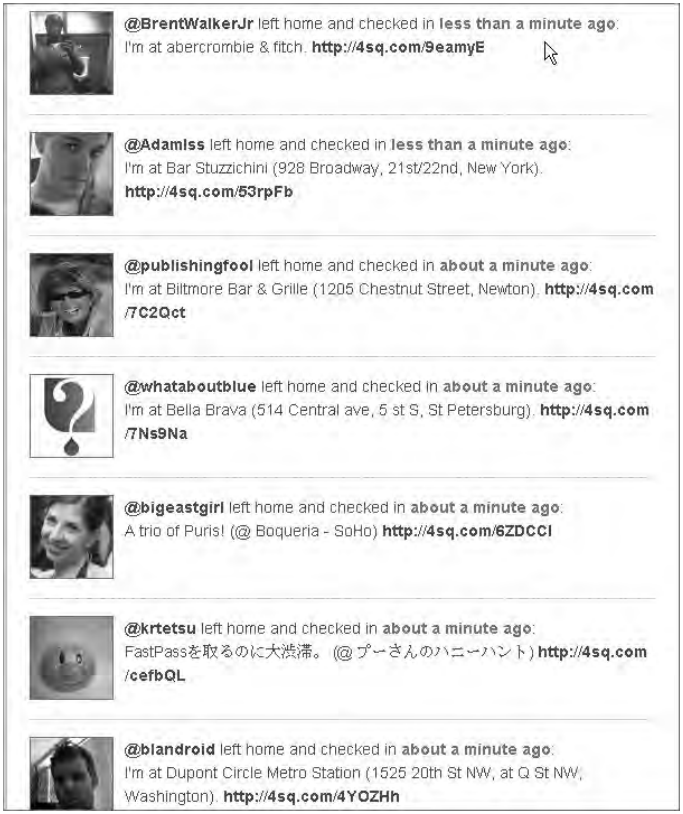



图2-4　ICanStalkU.com网站主页的经典场景

位置信息的泄露是社交网站令人不放心的因素之一。在上传照片的同时，你的位置信息可能在你毫不知情的情况下被泄露了。

像ICanStalkU这样的网站强调了信息泄露的危险。通过一则小故事（还有很多）便可以看到，这些位置信息如何被利用，使受害人遭遇入室盗窃和抢劫等，故事的链接如下：www.social-engineer.org/wiki/archives/BlogPosts/TwitterHomeRobbery.html。

不同种类的信息可以帮助你全面地了解目标。人们喜欢在Twitter上分享自己的地理位置、和谁在一起以及正在做的事情等。Blippy[①]能绑定人们的银行账号，然后向好友推送你的每笔消费信息，包括从哪里购买、花费多少等。含有地理位置信息的照片，以及Facebook这种用来分享个人照片、故事和其他相关信息的社交网站，是社会工程人员特别喜欢的信息源。只需片刻功夫，目标人物的住址、工作、照片、兴趣等信息就呈现在眼前了。

社交网站成为最佳信息源的另一个原因是可以匿名伪装。如果目标人物是一个刚离婚的中年男子，平时热衷于更新Facebook，那么你就可以假扮成一名希望结交新朋友的年轻女士。很多时候，人们在被拍马屁时，会泄露很多重要信息。结合伪装的技术，再加上人们通常认为自己见到、读到的就是真实信息这一安全漏洞，你便很容易得手。

#### 6. 公开报告

公开数据可能来自目标企业内部或者外部，包括季度报告、政府报告、分析报告及公开交易公司的收入信息等。例如，邓白氏集团（Dunn and Bradstreet）以及其他公司的销售分析报告都能以极低的价格买到，而这些报告中通常会包含目标公司的大量详细信息。

稍后会详细讨论的还有背景查询服务，比如www.USSearch.com和www.intelius.com。还有一些类似的有偿查询网站都提供查询服务，价格从每次1美元到49美元包月不等。通过搜索引擎，可以免费查到很多有用的数据，但一些财务明细数据和个人信息就得通过这种合法的付费形式有偿获得。最令人震惊的是，有些公司甚至会向客户提供个人的社会保险号（Social Security Number）。

### 2.2.2 运用观察的力量

虽然观察并不能称为社会工程工具，但是简单的观察却能给你带来关于目标的不少信息。目标企业员工使用钥匙、门禁卡（射频识别卡）还是其他方式进入办公大楼？有没有指定的吸烟区？垃圾桶有没有上锁？办公大楼有外置摄像头吗？供电系统或空调机组等外围设备的维修公司是哪家？这些信息都可以给社会工程人员的入侵提供可能。

上面仅仅是通过观察可以得出答案的几个问题而已。花上一段时间观察目标，并用隐藏式摄像机录制下来，然后回去慢慢研究和分析，你会学到很多知识并且你的信息量也会暴增。

① 一种消费信息分享网站，当你的朋友刷卡购物时，你能马上知道他们买了什么，以及这些东西的价格和购买地点。

## 2.2.3 垃圾堆里找信息

难以相信在垃圾堆里能找出让我们获利丰厚的信息，就像难以想象我们为什么要去乐呵呵地翻垃圾一样。人们经常会扔掉发票、通知、信件、CD光盘、电脑、U盘以及其他种类繁多的设备和报告，我们可以从中收集到特别多的信息。正如前面提到的，如果人们连价值数百万的艺术品都会扔掉，那么只要认为某物是垃圾，人们都会不假思索地直接扔掉。

有时，公司认为直接将重要文件扔掉会不安全，于是便用碎纸机碎掉再扔，然而一些碎纸颗粒度不高的碎纸机粉碎过的文件还是能轻易拼回去的。如图2-5所示。



图2-5　粗线条单向粉碎过的文件依然有些文字可读

这张图展示的是粉碎后的一些文件，有些字还是可以被整体辨认的。这种情况下，只要肯花时间耐心地用胶带黏一下（如图2-6所示），便能将部分文件拼接回去，从而得到破坏性极强的信息。

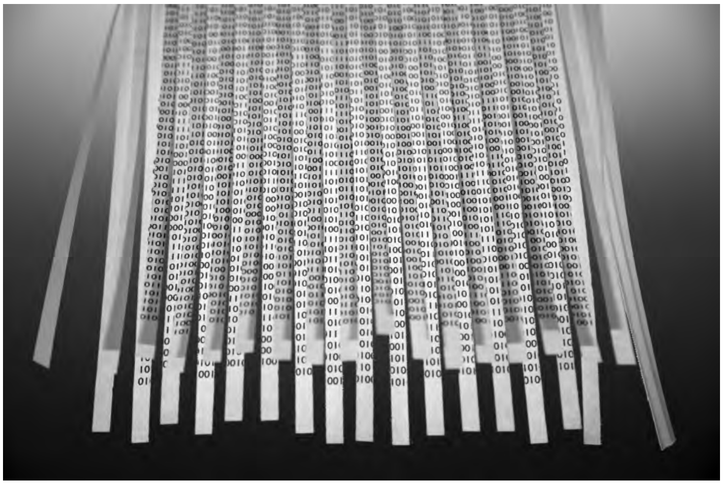


图2-6　只要肯花时间且有耐心，文档是能拼接回去的

不过，使用双向粉碎机进行销毁，就会粉碎得相当细，几乎不可能再拼接起来，如图2-7所示。



图2-7 很难想象粉碎前它是纸币

很多公司付费将已经粉碎了的文件交给专业公司焚烧。也有一些公司直接将粉碎完毕的文件丢给第三方处理，之后就不管不问了。你大概也能猜到，这样会令入侵者有机可乘。社会工程人员只要找到提供该服务的厂商，就可以轻而易举地冒充成过去收“垃圾”（粉碎过的文件）的工作人员。无论如何，翻找垃圾箱是一种快速收集所需信息的方法。不过，翻垃圾箱时一定要记住以下几点。

- **穿质量好的鞋子或靴子**。没有比跳进垃圾堆，然后被钉子戳到脚更令人抓狂的事了。确保你的鞋子合脚且鞋带系紧了，并能保护脚不为利器所伤。
- **穿深颜色的衣服**。这点不需要过多的解释。你肯定会穿那些丢掉也不会心疼的衣服，而且深色的衣服不容易被发现。
- **带一个手电筒**。
- **拿到了赶紧溜**。除非你是在偏僻到不可能被抓到的地方，否则最好是拿走一些垃圾袋，到其他地方去翻找。

翻找垃圾桶几乎总能找到一些非常有用的信息。只是有的时候，社会工程人员不需要去翻垃圾桶就能得到这些信息。第1章中有一个例子，详见http://www.social-engineer.org/resources/book/TopSecretStolen.htm。加拿大反恐部队计划建造一栋新的办公大楼，然而这栋大楼的一些规划蓝图被当做垃圾扔掉了，甚至都没有经过粉碎。蓝图中包括监控摄像头的安装位置、围栏及其他绝密信息。还好，发现这一图纸的人没有恶意，否则后果不堪设想。

正如该文章所写的，这则故事只是用来展示很多“愚蠢至极”行为中的一种，但是从社会工程人员的角度来看，翻垃圾桶确实是最好的一种信息收集方式。

### 2.2.4 运用分析软件

第7章将细致讨论社会工程人员会用到的专业工具集，这里仅作简单介绍。

Common User Passwords Profiler（“常用用户密码探查器”，缩写为CUPP）和Who’s Your Daddy

（“谁是你爸爸”，缩写为WYD）是两款常用的密码分析工具，社会工程人员可利用它们分析出企业或个人可能使用的密码。

第7章将深入讨论这些工具的使用方法。WYD这样的工具可以将个人或者公司网站上的信息收集起来，根据网站上涉及的词语来创建可能的密码列表。人们通常会使用文字、姓名或者日期作为密码。这种类型的软件能够轻而易举地生成密码列表。

像Paterva制作的Maltego工具（第7章有详细介绍），简直就是信息收集者梦寐以求的。这款工具本身就可以帮助社会工程人员完成基于网页的被动信息收集和查询工作，不需要借用其他任何平台或工具。

之后，Maltego可以存储这些数据并在屏幕上用图形化的方式展现，以用于报告、导出或其他用途。这些对于分析公司的信息相当有用。

记住，收集数据的目的是了解目标企业及其员工。一旦社会工程人员收集到足够多的数据，如何最充分地利用这些数据信息来操纵目标便会了然于胸。应该将目标公司作为一个整体来分析，了解里面的员工大致参加哪些俱乐部、他们的兴趣爱好或者加入的社团名称。他们会不会向特定的慈善机构捐款？或者他们的孩子都就读于同一所学校吗？这些信息对于深入分析都很有帮助。

清晰明了的分析不仅可以帮助社会工程人员很好地伪装，而且还可以让他们知晓要询问哪些问题，什么时候适合打电话及哪天适合当面交流等，还有会令攻击变得更加容易的很多其他线索。

前文提到的所有方法，大多是现实生活中手动的信息收集方式，并未涉及信息收集的技术层面，例如，简单邮件传输协议（SMTP）、域名服务（DNS）、网络基本输入输出系统（Netbios）和简单网络管理协议（SNMP）。第7章中细致地讲解了Maltego软件中有关上述信息的收集功能。这些方法值得探讨，但是技术性较强，并不是本书所关注的“人性”入侵技术。

逻辑上，无论使用何种方法收集信息，首先浮现在你脑海中的问题可能都是：既然知道收集信息的地点、方式以及分类、存储并显示此信息的方法，那么如何使用搜集到的信息呢？

作为一名社会工程人员，信息收集完成后，必须开始规划如何攻击。为此，首先要建立模型，列出信息使用攻略。交流模型的建立便是最佳的开始方式之一。

## 2.3　交流模型

> 交流模型越精巧、越清晰，花在交流上的时间就越少。
>
> ——约瑟夫·普利斯特利（Joseph Priestley）

交流是将信息从一个实体传送到另一个实体的过程。交流需要至少二者间的互动，可以视为一个双向的过程，这里发生着信息的交换、思维的碰撞、情感的互动，或者想法上的共识。

这个概念和社会工程的定义非常相似，只是这里假定参与交流的人已经有了一个共识，而达成共识是社会工程人员和他人交流的目的。交流可以理解为这样一个过程：信息经过打包，由发送者通过传输媒介送达接收者，接收者解密收到的信息并给发送者送去反馈。所有的交流形式都需要有三个条件：发送者、信息和接收者。社会工程人员理解交流的原理对于构建合适的交流模型异常重要。对于社会工程人员，建立交流模型将帮助确定最好的传送和反馈方法，以及最合适的传输内容。

交流可以采用多种不同的形式。有听觉方式，比如演讲、歌曲和说话的音调，还有非口头方式，比如肢体语言、手语、辅助语言、触摸和眼神交流。

不论使用何种交流方式，对于接收者来说，信息的内容及其传达方式都会有确切的效果。

理解最基本的规则对于为“目标”建立交流模型很重要。一些规则不可以被打破，比如交流总是有一个发送者和一个接收者。同时，每个人的实际情况都会因经验和观念的不同而有所不同。

基于个人的现实情况，人们对事情的感知、体验和阐释总是会有所差异。正因为这样，人们对同一事件的看法会不尽相同。如果你有兄弟姐妹，一个简单的练习就可以证明这一点。问他们对于一件事情，尤其是一个情感事件的解释或记忆，你会发现他们对这件事情的阐释和你的记忆是完全不同的。

每一个人都有身体和精神的私密空间。很多因素会影响你决定是否要允许他人靠近或进入这个空间。无论在何种场合，你和别人交流时，都是在尝试闯入他们的私密空间。社会工程人员的交流是尝试将他人带入其空间，从而了解他人的状况。有效的沟通是试图把所有的参与者带入彼此的精神空间。只要有互动，就会发生这种带入，只是这太普通了，一般人通常不会注意到这点。

人际交流会传送两个层次的信息：语言的和非语言的。

交流经常包括一个文字或语言部分，不管它是以口头、书面还是其他文字形式呈现。通常也会有一个非语言的部分——面部表情、肢体语言，或者情感、字体等一些非语言信息。

暂且不论每一种类型的暗示（语言或非语言）的数量，交流的信息包被传送给接收者，然后接收者根据其自身的情况进行过滤。他将根据其实际情况形成一个概念，然后根据这个概念来解释这个信息包。当接收者解释信息时，便开始整理它的意思，即使那个意思并不是发送者的本意。发送者只能通过接收者给的反馈信息包，确定对方是接受还是拒绝了这个原始信息包，从而得知其信息包是否以既定的方式被接收。

这里所说的信息包是指某种沟通方式，包括言语、信件或发送的电子邮件等。接收者收到信息时，就会去阐释它。许多因素会影响最终被阐释出来的结果，如情绪的好坏、喜怒哀乐等。所

有这些因素和改变接收者认知的其他暗示都将有助于他阐释该信息。

社会工程人员的目的是利用这些语言和非语言的暗示,改变目标的感知,从而达到想要的效果。

下面包含更多的基本交流规则:

- 不要理所当然地认为接收者和你的情况完全一样;
- 不要理所当然地认为接收者将按照你的方式阐释信息;
- 交流不是一个绝对的、一成不变的事情;
- 如果有多人参与交流,应始终假设每个人的情况各不相同。

知道这些规则可以极大地提高你和他人交流的效率。这很好,但是交流和建立模型有什么关系?或者说,这又和社会工程有何关系呢?

## 2.3.1 交流模型及其根源

正如前面所说,交流的基本含义是发送一个信息包给既定接收者。这些信息也许来自多个信息源,比如视觉、听觉、触觉、味觉和语言。这个信息包随后被接收方处理,用于描绘出对方"所说的意思"。这种评估方法就是所谓的通信过程。通信过程最早是在1947年由社会科学家克劳德·香农(Claude Shannon)和沃伦·韦弗(Warren Weaver)提出的。当时他们发明了香农–韦弗(Shannon-Weaver)模型,也被称为"鼻祖模型"。

根据维基百科的定义,香农–韦弗模型"包含了信息源、信息、发送器、信号、信道、噪声、接收器、信息目的地、误差概率、编码、解码、信息率和信道容量等概念"。

香农和韦弗用图像定义这种模型,如图2-8所示。

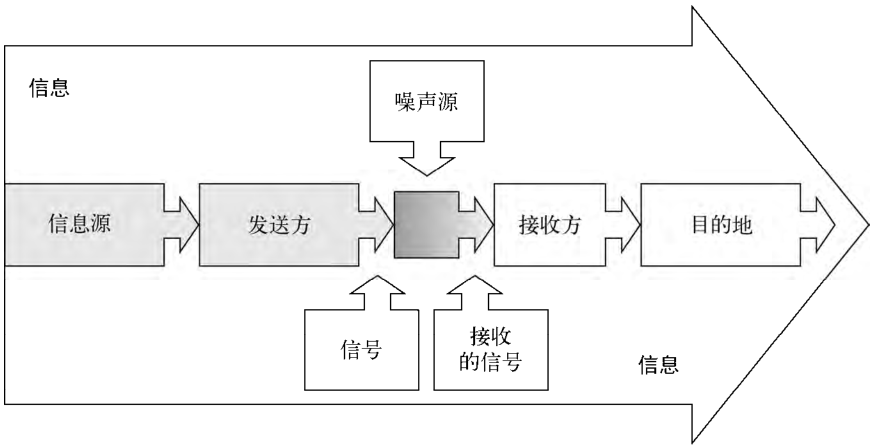



图2-8 香农–韦弗的"鼻祖模型"

在这样一个简单的模型（也被称为传递模型）中，信息或内容从发送者那里以某种形式发送到目的地或接收者那里。通信这一基本概念只是将通信视为发送和接收信息的一种方式。该模型的优势在于简单、通用和可量化。

香农和韦弗构建这个模型的基础如下。

- 一个创造信息的信息源
- 一个把信息编码为信号的发送方
- 一个适合传送信号的信道
- 一个从信号中解码（重构）出信息的接收方
- 一个信息发送的目的地

通过这一理论，他们总结出通信中存在的3个层面的问题。

- 技术问题——信息传送的准确性如何？
- 语义问题——信息表达的精确性如何？
- 效率问题——接收到的信息对行为影响的有效性如何？（社会工程过程中这最后一点很重要，必须牢记。社会工程人员的目的就是创造出一个自己想要的行为。）

差不多15年以后，大卫·贝罗（David Berlo）扩充了香农–韦弗的线性通信模型，发明出发送者–信息–信道–接收者（SMCR）通信模型。SMCR将模型分解成几个清晰的部分，如图2-9所示。

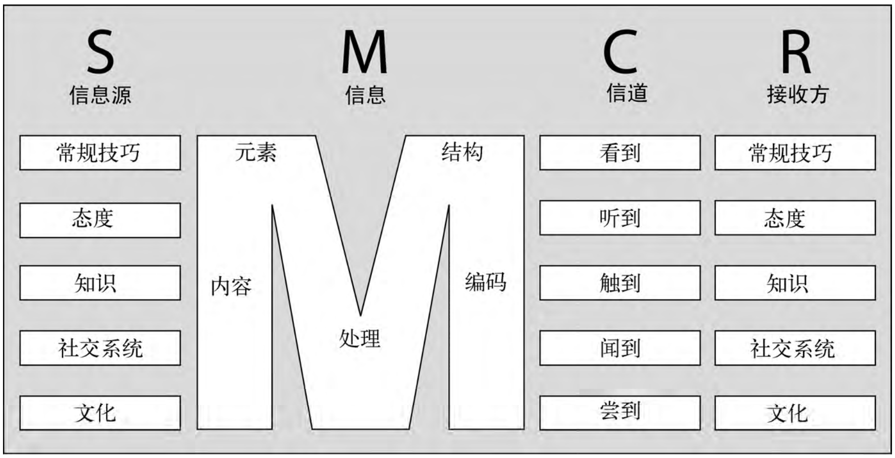



图2-9　贝罗模型

可以认为通信是信息传播的过程，该过程由3个层次的规则控制。

- 符号和标识的形式属性
- 符号/表情及其使用者之间的关系

- 符号和标识间的联系及其含义

因此，可以进一步地将通信定义为社交，即至少两个对象使用一系列共同的符号和规则进行互动。

2008年，另一位研究员D. C. 巴尔芒（D. C. Balmund）将自己的研究与行业先驱的成果结合起来，形成了通信的事务模型，如图2-10所示。

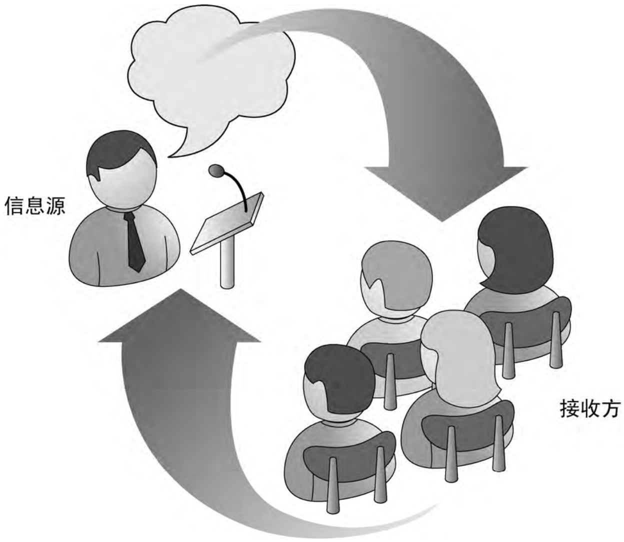



图2-10　改进的新通信模型

在他的模型中，可以看到信道和信息可以有多种形式，不仅是图片中所示的口头语言。信息可以有书面、视频或音频等形式，接收者可以是一人或多人，反馈也可以有多种形式。

将这些成果结合起来进行研究有助于社会工程人员制定出一个稳健的通信/交流模型。不仅是社会工程人员，每个人都可以从中获益。学习如何制订交流计划可以加强你和他人（例如配偶、孩子、上司或下属）之间的交流。

因为本书的重点是社会工程人员，所以需要分析一名社会工程人员可以从中学到什么。在读完该理论所有内容之后，你可能会困惑于怎么使用这些理论。请记住，社会工程人员必须是交流的大师，必须能够有效地进入且留在一个人私密的精神空间，并保证不冒犯目标或令目标反感。制定、实现和实践有效的交流模型是成功的关键。那么，接下来我们就学着制定这样一个交流模型。

## 2.3.2　制定交流模型

既然已知晓交流模型的关键要素，请以社会工程人员的视角来看待这些要素。

- **信息源**：社会工程人员就是要传递的信息或交流的源。
- **信道**：就是传达方式。
- **信息**：向接收者传达的内容。
- **接收方**：即目标。
- **反馈**：当有效地将信息传达出去之后，你希望对方给予的回应。

如何有效地使用这些要素呢？运用交流模型的第一步是带着目的动手实践，首先从社会工程中上演的经典剧情开始。

- 编写一个网络钓鱼邮件，尝试让25~50个雇员在工作时间访问一个嵌有恶意代码的非商业网站，以达到入侵其公司网络的目的。
- 登门拜访，伪装成一个前来面试的人员，装作不小心将咖啡洒在了简历上，并说服前台工作人员允许你用USB存储器插入到电脑里重新打印一份。

在制定交流策略时，你可能会发现反向使用模型大有裨益。

- **反馈**　你期望得到什么样的回应？期望的回应是，接收邮件的大部分雇员都点击它，这是理想状况。当然，只有少数甚至一个目标人物点击你也会感到高兴，但是你的目的，即期望的反馈是让大部分目标人物上当。
- **接收方**　这就是信息收集技巧派上用场的地方。你需要知道目标人物的全部信息。他们喜欢运动吗？他们中大多数是男性还是女性？他们是当地俱乐部的会员吗？休息的时候他们做些什么呢？他们成家了吗？他们是否年轻？这些问题的答案有助于社会工程人员决定传达什么类型的信息。
- **信息**　如果目标人物主要是25~40岁的男性，并且有几个人是足球或篮球联赛的球迷，那么目标人物就可能会点击运动、女人或者是赛事相关的链接。制定邮件的内容是很重要的，但也要仔细考虑语法、拼写及标点符号等。根据以往的经验，拼写不规范是网络钓鱼邮件露馅的主要原因之一。

  如果收到的邮件内容是“点击这里，输入尔的密码来验证尔的账户设定”，那么内容不正规就是其致命的问题。邮件必须拼写规范并且能够吸引目标人物的注意。即使目的相同，根据目标人物的性别、年龄或其他因素的不同，内容也应有所变化。如果目标主要是女性，发送同样的邮件就很可能会失败。
- **信道**　这个因素的答案很简单，因为你已经知道是用邮件作为传输方式。
- **信息源**　同样，这个因素你也无需费神，因为作为一名社会工程人员，你就是信息源。你的可信度取决于你作为一名社会工程人员的技术水平。

**场景一：网络钓鱼邮件**

目标人物是45名25~45岁的男性，其中有24名是梦幻篮球联赛的球迷，他们每天都会访问网站www.myfantasybasketballleague.com来进行投票。这些信息是通过论坛上的投票证实的。

我们的目的是要他们去访问一个归你所有的且可访问的网站 www.myfantasybasketballeague.com，该网址和他们经常访问的网址只有一个字母之差。从外观上看，这个网站是他们访问的那个网站的克隆，两者只有一点不同，即这个里面有个内嵌的恶意帧。网页中间会有个登录按钮，点击之后，会返回到真正的网站。在点击和加载之间的延时，嵌入的代码会入侵他们的系统。

怎样写这封邮件呢？下面是我写的一个范本。

> 你好！
>
> 这是来自“我的梦幻篮球联赛”的好消息！我们新增了一些功能，用户能够在投票时拥有更多的控制权，此外还有一些特殊的功能。我们正努力将这些功能提供给所有的会员，但是需要增收部分服务费。
>
> 我们很高兴地告诉你，前100名登录的会员可以免费享受这项全新的服务。点击邮件中的链接，到我们的活动页面，然后点击网页上灰色的登录（LOGIN）按钮进行登录，就可以将这些功能添加到你的账户中。网址为www.myfantasybasketballeague.com。
>
> 谢谢！
>
> 我的梦幻篮球联赛团队

这封邮件至少会使那24名联赛球迷感兴趣，诱导他们去点击链接，查看网站并且免费试用这些功能。

分析一下这封邮件。首先，它有一个吸引梦幻篮球联盟网站现有会员的邀请。然后，他们中的很多人会意识到这个邀请只限定给前100名，所以一收到邮件就会点击链接，而且很可能还是在工作期间。邮件链接的网站含有恶意代码，虽然大部分人会成为受害者，但是只要有一人落入圈套，社会工程人员的目的就已达到。

同样需要注意的是邮件的语法及拼写都是正确的，一个诱人的“钩子”和足够的诱惑力让人快速点击。这就是一封完美的钓鱼邮件，它的基础便是坚实的交流模型。

**场景二：USB存储**

现场进行社会工程要困难一些，因为是面对面进行的。当着目标的面，你只能“伪装”自己。你必须记住所有的细节，因为现场没有退出或者看提示的机会。要记住，我们往往只有一次机会打动别人，这一点很重要。如果这一出搞砸了，接下来也就不用再演了。

> **反馈**　这个场景的目的是让前台接待员接受你的带有恶意程序的U盘。在U盘插入电脑后，该程序会自动加载并提取系统中所有与账户相关的信息，比如用户名、密码、电子邮件账户以及包含系统中所有账户密码的SAM文件等，然后将这些数据复制到U盘指定

的目录下。同时，从前台的机器创建一个反向连接到你的服务器，从而获得该机器甚至公司网络的访问权限。我喜欢使用Metasploit Framework或者能够和Metasploit搭配使用的社会工程工具（见第7章）。Metasploit可以在受害主机上执行破坏性代码，并且有一个内置的Meterpreter处理工具。使用者可以通过编写脚本完成许多工作，包括键盘记录、屏幕截图及获取受害者电脑的信息等。

- **接收方**　有一个特定的攻击对象时，会感到棘手，因为如果想法不被目标所接受，那么你的计划就没有什么胜算了。你必须热情、友善，且具有一定的说服力。建立信任的过程也必须很迅速，因为时间太长将会让目标起疑心。但是如果处理得太快了，也会引起忧虑和害怕，从而失去机会。所以必须找到一个完美的平衡点。
- **信息**　因为你是面对面地传送信息，所以必须简洁明了。故事的基本内容如下：你在报纸上看到关于招聘数据库管理员的广告，然后打电话给人力资源部门的黛比。她说今天有预约了，但是你可以先把简历送过去，本周晚些时候再进行面谈。在你开车过去的时候，一只松鼠跑了出来，导致你急刹车，使得咖啡洒了出来，溅到了包上，弄脏了简历和其他物品。同时，你还有另外一个约会，但是又很需要这份工作，希望她能够通过你的U盘重新打印一份新简历。
- **信道**　面对面的口头交流，运用声音、面部表情和肢体语言。
- **信息源**　再强调一次，作为社会工程人员，你就是信息源，除非你觉得有必要找一个替身。

手中拿着沾上咖啡渍的文件夹，里面装些湿的文件，会使故事更加逼真。沮丧而无助的表情也会很有帮助。说话的时候要有礼貌并且真诚，以博得她的好感甚至同情。U盘中要有可打印的myresume.doc文件或myresume.pdf文件。PDF是最常用的格式，大多数公司会运行有漏洞的较老版本的Adobe Reader程序。确保简历不是一些特殊的格式，能被大多数人打开。

> 大多数时候人们会伸出援助之手。如果情节真实感人，他们会愿意帮助那些遭遇不幸的人。如果你缺少社会工程人员的天赋，我给你一个特别的建议，你可以在故事中加入这么一段：我今天过来顺路送女儿上学，她在爬过椅子和我吻别时，不小心将咖啡打翻洒进了我的包中。我当时已经离家比较远了，而且要迟到了，来不及回去。您能帮忙重新打印一份吗？

无论如何，这个故事通常都会成功，前台会将U盘插入她的计算机，导致计算机被入侵，我们也就成功入侵了公司的网络。

## 2.4　交流模型的力量

交流模型是一种很强大的工具，每个社会工程人员都必须掌握。交流模型中最困难的部分是确保收集到的信息是可靠的。

在前面提到的两个场景中，计划和模型准备不充分都将会导致失败。练习交流模型的一个好办法是写下一个操纵熟人（丈夫、妻子、父母、孩子、老板或者朋友）的模型，让他们按照你的想法和希望来行动。

设定目标，但不要怀有恶意，例如，使某人同意改变度假地点，或者说服同伴去你喜欢而他讨厌的餐馆吃饭，或是允许你买一件你通常不会去买的东西。不管你的目标是什么，将5个交流要素写出来，看看在具有书面计划的时候，交流的情形如何。你会发现在目标清晰的情况下，能更好地检验社会工程的交流方法，也更容易实现目标。依次列出如下的5点要素，并逐个填写好，然后在实施过程中将其关联起来。

- 信息源
- 信息
- 信道
- 接收方
- 反馈

交流模型能引出许多非常有价值的信息，没有它，社会工程人员的大多数行动都会失败。就像前面提到的，信息收集是社会工程的关键，但是如果只精通收集信息，却不知如何运用信息，那么终不过是白忙一场。

学习成为一名信息收集大师，然后与交流模型相结合予以实践。这只是个开始，但是它能改变你作为社会工程人员及在日常生活中与他人交流的方式。不过，要构建交流模型中的可靠信息，还有更多知识等待我们去挖掘。

学会如何提问是进行沟通、操纵他人乃至最终成为社会工程人员的关键所在，这方面的知识将在下一章中进行讨论。

# 第 3 章

# 诱　　导

不战而屈人之兵，善之善者也。

——孙子

有效地引导别人将心里话说出来，是社会工程成功的关键。在人们见到你并和你交流时，你应该让他们感觉很自在，使之主动吐露心声。

你是否碰到过什么人，然后立刻觉得“哇，我喜欢这个人”？为什么会这样呢？他究竟有什么特质让你有这种感觉呢？是他的微笑，他的长相，他对待你的方式，还是他的身体语言？

或许是他与你的想法及期望值比较“一致”。他看你的眼神比较平和，没有偏见，你便立刻觉得和他在一起很放松。

现在设想你也有这样的潜力并能掌握这种能力。不要以为本章只是讲讲“怎样构建友好的关系”，因而置之不顾。本章讲述的是诱导。诱导是间谍、骗子和社会工程人员常用的一种强大的技术，医生、治疗师和司法人员也在使用。如果你希望保护自己，或者希望成为一名优秀的社会工程审计人员，那么就必须掌握这一技巧。有效地使用诱导会产生惊人的效果。

什么是诱导？它是社会工程中少有的几个强有力的工具之一，这也是将它置于社会工程框架顶层的原因之一。仅通过这一种技巧，就能改变人们对你的看法。从社会工程的角度来看，它能改变你在安全实践中的工作方式。本章将详细分析几个专业诱导的实例，深入分析这一技术在社会工程场景中的应用。

千里之行始于足下，我们还是得从基础开始。

## 3.1　诱导的含义

诱导的意思是引出、套出或者得出一个逻辑上的结论（例如某种事实）。或者，可以将诱导定义为一种引发或者诱发某种特定类型行为的刺激，正如“诱导他说出供词时颇费周章”一句中的意思。

请再看一遍上面的定义，如果没有起鸡皮疙瘩的话，那么你的理解就有问题。想想它的含义。有效地使用诱导意味着你能提出具有诱导性的问题，刺激别人采取你所希望的行动。对于社会工程人员来说，这意味着有效地使用诱导可以将你说话及提问的技能提升到一个全新的层次。从信息收集的角度来讲，专家级的诱导就是指目标愿意回答你的任何问题。

我们再深入一些，因为全球的间谍都会使用诱导技巧，所以很多政府部门会对其公职人员进行培训并给出警示，以对抗诱导。

在美国国家安全局的培训材料中，对诱导的定义如下：在貌似正常和平凡的对话中精妙地获取信息。

这样的会话可能发生在任何地方，比如餐馆、健身房及托儿所等。诱导使用起来效果很好，因为其风险较低且通常很难被察觉。大部分情况下，目标甚至不知道什么时候泄露了信息。如果被怀疑动机不纯，则可以“不过随便问个问题”为由假装生气、蒙混过关。

诱导的效果如此之好的原因如下：

- 大部分人希望看上去比较有礼貌，尤其是对陌生人；
- 专业人士希望自己看起来见多识广、很有才气；
- 如果得到赞赏，大部分人通常会越说越起劲并泄露更多的秘密；
- 大部分人不会为了撒谎而撒谎；
- 大部分人对貌似关心自己的人会比较友善。

大部分人都有这些特点，这使得诱导的成功率极高，也使得人们在说起自己的成就时口无遮拦。

有一次，我的任务是收集某公司的内部资料，我在当地举办的一次商业会议活动中碰到了目标。现场人比较多，我一直在寻找机会，后来终于发现目标走向吧台，于是我也在同一时间走过去。这类会议的目的就是要交换名片、结识更多的人，所以我主动上前打招呼并不会显得冒昧。

我说：“清静片刻？”

他笑着回答：“是啊，还好有这个地方，可以坐下来喝点东西。”

听到他点什么饮料后，我也点了一杯类似的。我伸出手，说道：“我叫保罗·威廉姆斯。”

“我叫拉里·史密斯。”

我拿出准备好的在网上定制的名片，说：“我是一家小型进口公司采购部的经理。”

他也拿出名片递给我，说：“我是XYZ公司的首席财务官。”

我笑着说：“你是管钱的啊，怪不得每个人都在那边围着你。你们公司具体是做什么的？”

他开始说起公司一些产品的情况，当说到一个知名产品时，我说：“哦，原来是你们公司做的啊，我喜欢那个产品。我在《XYZ杂志》上看到过，好像创造了销售记录啊。”我从之前收集的信息中了解到，他个人也很喜欢那个产品，所以我的赞美会起作用。

这时他开始显得有点骄傲了：“你知道那个设备在第一个月的销量就超过了它前后5个产品的销量总和吗？”

“是啊，我知道为什么，因为我自己买了5个。”我笑着附和。

经过一段时间，又喝了一杯之后，我了解到他们最近购买了财务软件、最近在度假的首席安全官的名字，以及拉里不久也要和太太一起到巴哈马度假。

这些看似无用的信息可不是毫无价值。我得到了关于他们的软件、人员和度假的详细信息，这在我计划攻击时会很有帮助。但是我没有满足，而是提出了一个更深入的问题：

“我知道这个问题会很怪，但是我们是个小公司，老板让我研究并购买一套门禁系统。我们现在使用钥匙，但是他认为RFID或者类似的系统会更好。你知道你们公司用什么吗？”

这个问题很敏感，会引起一般人的警觉。没想到他却说：“这个我可没有概念，我只负责签支票购买，不过我进门时使用的就是这个小卡片……”他拿出钱包中的卡片给我看。“我想可能是RFID，不过我只知道进门时晃一下钱包，门就开了。”

我们一起笑了起来，这些信息对我的攻击来说太有帮助了，我满载而归。你们可能注意到了，诱导与信息收集很相似且紧密关联。通过良好的伪装（第4章介绍）和诱导技巧，这个特别的信息收集过程会容易得多。诱导技巧的应用使得问题能够自然地提出，目标在回答这些问题时也觉得很自然。

了解到拉里正在度假中、他们公司使用的财务软件类型以及门禁系统，我就可以策划一次修复“故障”RFID打卡机及出勤记录钟的行动。我与前台的沟通很简单：“拉里在到巴哈马度假之前打电话给我，说生产部门有一个出勤记录钟没有正确注册，我来测试并分析一下，只要几分钟就可以完成。”前台连问都没有问，就让我进去了。

诱导所得到的信息使得前台接待人员对我伪装的角色没有丝毫怀疑，我成功地进入了目标单位。

通过简单、轻松、愉快的谈话就可以从很多人手中获取最好的信息。讨论到现在可以发现，重要的是为了实现最佳结果而明确定义你的目的。诱导不仅用于信息收集过程，也可以强化你的角色伪装，从而获取信息。所有这些成果依赖于定义清晰、经过深思熟虑的诱导模型。

## 3.2　诱导的目的

请回顾一下诱导的定义，其中清晰指明了你的目的。不过，你可以将其归纳成一条。社会工程人员想要目标对象做某件事，这件事可能简单到只是回答一个问题，也可能复杂到允许他进入一个限制区域。要达到这一目的，社会工程人员需要询问一系列的问题，或者与目标对象进行交谈，最终引导目标对象帮他达到目的。

信息是其中的关键。获取的信息越多，攻击的成功率就越高。因为诱导不具有威胁性，所以很容易成功。请想想一周中你在商店、咖啡馆或者其他地方进行过多少次无意义的短时谈话。谈话的真谛在于使用诱导战术，并且每天都以一种无恶意的方式使用。这也是诱导有效的原因。

在英国当红真人秀节目《骗术真相》的一期节目现场，主持人展示了社会工程攻击是多么地容易。这期节目中，攻击的目的是吸引目标对象参与一个被操控的撞大运游戏。为此，攻击者的一个同伴扮演成陌生人，与攻击者交谈，并且在谈话中表现出极大的兴趣。谈话吸引了周围的人，这样就很容易诱导目标，从而得到所期望的响应。这种方法屡试不爽。

不管采用何种方法，目的都是获取信息，随后利用这些信息引导目标采取社会工程人员所期望的行动。理解这一点很重要。后续章节还会介绍伪装以及其他操纵策略，但不要将它们和诱导相混淆。要意识到，诱导需要通过交谈实现，这一点很重要。虽然它和伪装、肢体语言以及眼神密切相关，但是相较于在谈话中进行的诱导来说，这些活动稍显逊色。

一些专家认为掌握交谈的艺术需要3个主要步骤。

(1) *表现得自然*。如果在交谈中显得不舒服或者不自然，会很快导致谈话失败。要想验证这一点，可以进行如下练习。与他人谈论一些你精通的领域，在这个过程中你可以录像或者让朋友观察，观察你的站姿、动作以及阐述知识的方式。这些行为可以反映出你的自信和自然。然后，尝试参与一些你一无所知的领域的谈话，同样进行录像或者让朋友观察。看看在这种对话中你试图发表“真知灼见”时，这些非语言方面有哪些变化。

这些练习会显示出你表现自然与表现不自然的差异。与你交谈的人很容易就会察觉这一点，不自然的表现会葬送你成功诱导的机会。如何在谈话中表现得自然？我们来看第2步。

(2) *拥有足够的知识*。你必须了解与对象交谈时所涉及领域的知识。本部分应该带有一个巨大的红色警告标志，但是书本中不能有这样的标志，所以我就强调一下：

*最要紧的*是你不能装成自己不可能成为的人。

有点疑惑？举个例子分析一下。如果要得到某个绝密产品的化学成分，你要诱导的目标是制造该产品的一位化学家，并且决定和他谈论化学，那么此时你不能伪装成一个世界级的化学家（除非你真是）。他可能在交谈中提出一些你一无所知的问题，那样你就演砸了，诱导行动也就归于失败了。

更加现实的方式是伪装成一个学习某专业的学生，得知他在这个领域有惊人的造诣。基于他的专业知识，你只是要问他一个与自己正在研究的化学分子式有关的问题，问他该分子式为何没有效果。

重点是，不管你选择谈论哪个话题，也不管你选择和谁交谈，都要做些研究、反复练习且精心准备。一定要具备足够的知识，就目标对象会感兴趣的话题侃侃而谈。

(3) 切忌贪婪。当然，诱导的目的是获取信息、得到答案或者取得进入某领域的钥匙。然而，不要将此作为重点。如果你一心想得到自己需要的信息，很快就会被目标看穿，导致目标失去兴趣。通常情况下，给对方一些感兴趣的东西会引起对方的交换情结（第6章会讨论），这样对方会觉得有义务给你一些回报。在交谈中这一点很重要。交谈中要有来有往，除非对方是一个滔滔不绝的人。如果他谈论不止，就让他说。如果你得到了一些信息，就适可而止，不要贪婪地不断深挖，否则会引起对方的警觉。

有时，世界上的“最佳交流者”其实是那些听的比说的多的人。

这3个成功诱导的步骤能有效改变你和其他人在日常生活中的交流方式，不仅对社会工程人员和安全审计人员有益，对普通人也是如此。我个人想在这“3个步骤”上再加1~2步。

例如，交谈中诱导的一个重要方面是面部表情。表现得太紧张或太放松都会影响人们对你问题的反馈。如果你言辞镇定，并且吸引了目标参与交谈，但是身体语言或面部表情却表现得漠不关心，这会影响对方的情绪，即使他自己并没有意识到这一点。

下面这个例子可能稍显突兀，但我是塞萨尔·米兰（Cesar Milan，也称“狗语者”）的粉丝。我认为他是个天才。他可以与那些难以驯服的狗沟通。仅仅只需要几分钟时间，他就能让狗和其主人产生一种特质，从而让他们形成亲密的关系。他主要是教授人们怎样与狗沟通，即怎样通过狗可以理解的语言要求或告诉狗去做某事。他的理论中有一点我很认同，就是人的“精神”或活力会影响狗的精神或活力。换句话说，如果一个人走近狗的时候处于精神紧张且焦虑的状态，那么即使他的言辞显得很镇定，狗也会紧张、狂吠甚至具有攻击性。

显然，人和狗是不同的，但我认为上述理论同样适用于人。当社会工程人员接近目标时，他的精神或活力会影响对方的感知。活力会通过肢体语言、面部表情、穿着打扮等各方面表现出来，语言只是一种辅助的表现方式。在不知不觉的情况下，人们就会有所感知。你有没有想过或者听别人说过，“那家伙似乎很猥琐”或者“这姑娘看上去很友善”？

这背后的原因是什么？一个人的精神或活力会传递到你的“感知器”，这些数据会和以往的经历相关联，从而形成一个判断。判断会立刻形成，很多时候连自己都不知道。所以在进行诱导工作之前，必须使你的活力与所扮演的角色相匹配。如果你的个性或精神特质不能使你轻易伪装成一位经理，那么就不要尝试去这么做。必须找到适合你的角色和切入点。就我个人来说，我只是一个普通人，强项不在化学或高等数学上。如果要参与化学和高等数学方面的对话，我不会扮演一个对二者十分精通的人，而是会伪装成一个只想随便聊聊天气的陌生人。

不管你选择使用何种方法，都需要做一些准备工作，以期得到更好的结果。其中的一个步骤可以称为铺垫。

### 3.2.1　铺垫

排队买10美元一张的电影票时，会看到很多即将上映的影片的海报。等到你排队买40美元的爆米花和饮料时，会看到更多的海报，然后一路挤到自己的座位上。最后，电影正式开始前，还会放映一系列影片的预告片。有时，有些影片还没有开始制作，广告和预告片却已经到处都是，广告中可能会说“这是自……以来最有趣的影片”，或者随着一段恐怖的音乐响起，屏幕上烟雾弥漫，画外音提示“你认为‘少年杀手第45部’已经结束了……”，极尽精彩之处。

不管是什么电影，营销攻势都会告诉你如何去感受电影，换句话说，也就是在试映之前通过铺垫植入你应该对电影产生的看法。通过两三分钟的预告短片显示影片的概貌，让你产生看这部电影的意愿，并且呼吁那些想看喜剧片、恐怖片或爱情片的人前去观看。

虽然之前关于铺垫的文章不多，但这是一个严肃的课题。铺垫意指你可以按照它说的做——通过植入的信息或观点影响目标对特定信息的反应。铺垫常用于营销信息中，例如一些全国性连锁餐馆会通过广告展现人们微笑着享用美食，食物看起来精致而完美。当画面中的人说“太好吃了！”或者“哇噢！”的时候，你似乎也能感觉到其中的美味。

当然，社会工程人员不能通过商业广告来影响目标，那么如何在社会工程过程中应用铺垫技术呢？

在大多数社会工程应用中，你得从最终结果出发，确定开始时应该做哪些准备工作。你的目的是什么？你诱导的一般目的可能是获取对象工作项目的信息，或者他在办公室/度假的时间。不管是什么，必须首先设定目标。接下来要决定你要问何种类型的问题，然后才能决定如何植入一些前期信息，诱使对方给出你想要的答案。

例如，晚上你想要去某个地方吃牛排，但是喜欢使用折扣券的妻子并不喜欢那家餐馆，而你却时时刻刻想着那些肋眼牛排，此时就可以通过意念植入来影响对方。早晨你可以无意中说起：“亲爱的，你知道我在想什么吗？一块大大的、鲜嫩多汁的烤牛排。前几天我开车去邮局，看到邻居弗雷德将烧烤架放在路边，用木炭烤牛排，香气从车窗飘进来，从那以后我就一直想吃牛排。”

这个时候，妻子对这个诱导有没有反应并不重要，你已成功植入了一个思想的种子。她会设想牛排在烤架上滋滋作响，然后你接着说烤牛排的过程，说弥漫的香气，说自己有多么想大快朵颐。

如果接着你带了份报纸回家，浏览中发现有目标餐厅的广告，上面有折扣券。只要将折扣券页面折叠放在桌上即可。当然，你的妻子可能看到，也可能没看到。但是，因为你把它和信件放在了一起，之前提到了牛排，而且她喜欢折扣券，所以桌上的折扣券会引起她的注意。

过一会儿，她可能会过来问你："今晚想吃什么？"这就是你之前一系列铺垫工作所发挥的作用——你提到了飘香四溢、鲜嫩多汁的牛排及自己的渴求，你将目标餐厅的折扣券放在桌子显眼的位置上，现在是晚餐讨论时间。你可能会回答："今晚如果在家里吃的话，你不仅得做饭还得花时间清理，我们已经有段时间没去XYZ牛排馆了，今晚我们去那里如何？"

因为你知道她不喜欢那个餐馆，所以希望之前的铺垫工作能发挥作用。她回答道："我看到报纸上有那个餐厅的折扣券，第二份半价，但是你知道我不喜欢……"

在她说的时候，你可以用赞赏的语气插话："哈！折扣女王再次出击。我知道你不大喜欢牛排，但是我听莎莉说那边的鸡肉也很棒。"

几分钟之后你就会在去那个餐厅的路上。如果没有前期准备工作，你很可能会得到干脆的拒绝："不去。"铺垫工作对她的思维产生了影响，使她接受了你传递的内容并最终发挥了作用。

再看另外一个非常简单的例子。一个朋友走过来说道："我告诉你一件特别有趣的事情。"你会怎么反应呢？可能在他说出之前你就开始微笑了，你期待一个好玩的故事，所以在等待一个大笑的契机。他对你进行了铺垫，使你对幽默故事无限期待。

在社会工程领域如何应用这些原理呢？

铺垫本身就是一种技巧。以一种隐晦或婉转的方式植入想法或思路，比诱导本身更需要技巧。根据目标的不同，铺垫有时是相当复杂的。前面牛排的场景就是一个复杂的问题。铺垫需要投入时间和精力，特别简单的铺垫可能就是找出对象开的是哪个品牌的车或者其他一些看似无关紧要的信息。你可能"碰巧"与目标处于同一家熟食店，于是开始一次随意的聊天，你说道："哥们，我很喜欢自己的丰田车。刚刚在停车场有个开雪佛兰的家伙倒车时撞了我的车，结果连个划痕都没有留下。"如果足够幸运的话，你对丰田车的评论会引起对方的兴趣，随后你们可能会讨论车型或你想了解的其他话题。

在开始分析如何利用诱导的同时，考虑铺垫的问题会更有意义。社会工程人员从一开始就掌握了这一技巧。很多时候，社会工程人员在开始社会工程生涯之前就已经意识到自己有该项技能了。他们在青少年时期就发现与人沟通很简单，并且随后会倾向于与人沟通的工作。也许他是所在朋友圈的中心，人们遇到问题时会找他倾诉，会和他谈论任何问题。他后来意识到这些交流技巧能让他得到很多别人不能获得的机会。

我年轻时就具有这一天赋。父母经常说起，我在五六岁时就能和完全陌生的人交流，有时我会走进繁忙的餐厅厨房，询问我们订单的情况或者菜是怎么做的。不管怎样，我做到了这一点，为什么呢？也许是因为我根本不知道这种行为的怪异，因为我非常自信。在我长大后，这种天赋（或者无畏精神）得到了更全面的发挥。

似乎人们（有时甚至是完全陌生的人）喜欢向我倾诉他们遇到的难处，喜欢和我交流。十七八岁时发生的一个故事可以说明我在利用铺垫以及诱导技术方面的技巧。

我曾经非常热衷于冲浪，所以经常会做一些奇怪的工作以支撑这一爱好，从比萨快递员、玻璃纤维切割师到救生员等不一而足。有一阵，我给父亲的财务咨询公司做些杂事，经常递送文件给他的客户，待客户签好名后再拿回来。很多客户会和我聊起来，聊他们的生活、离婚以及生意上的起起落落。通常，开始时他们仅仅是告诉我，我父亲对他们来说是如何重要。当时我很难理解，为何人们，尤其是成年人，会向一个十七八岁的年轻人敞开心扉，讲述其生活的艰辛。

有一个我经常拜访的特别的客户，他拥有一整幢复式公寓，不大也不豪华，他只是拥有并管理着这些资产。这个可怜的家伙问题真多：家庭问题、健康问题及个人问题。每次只要我一坐下来他就开始反复不停地说。从那时起我就发现，只要坐在那里听就可以了，同时我可以神游于物外或者做一些奇妙的事情。这让他们感觉自己很重要，也显得我是一个乐于倾听的好人。我完全可以坐在那里遐想下一次美妙的冲浪，关键是我给他的感觉是在倾听。

通常我会一直听，直到受不了他所喷出的“浓烟”（他抽烟比我所见到的任何人都要多）。因为我还年轻，没有经验，所以无法提出什么建议，也没有什么解决方法，只有耳朵。关键是我真的关心，并未假装，我真心希望能有一个解决方法。有一天他告诉我，他很想回到西部，他的女儿在那里，他可以离家人更近一些。

我当时正想有些变化，换个更酷且更有趣的工作，挣更多的钱，以便买更好的冲浪板和其他“需要”的东西。在一次倾听过程中，我突然冒出一个疯狂的想法，而且他也认为我是一个有责任心、有激情而且还有些头脑的年轻人。前几个月的促膝交流和倾听建立了良好的铺垫基础，现在是收获的好时机。我说：“你回去吧，这边的物业由我帮你打理如何？”这个主意很荒谬，现在回过头来看，我会嘲笑这个古怪的想法。但是我和他交流的时间加起来有好几周，甚至有几个月了，我一直在倾听他的问题，我了解他以及他的痛楚。此外，我从没有过类似嘲笑或贬低他的做法。现在，他和我分享自己的问题，而我提供了一个对他来说可能很完美的解决方案，我们可实现双赢。我在收入方面的要求不高，他也想离家人更近一些。我们通过前面几个月的沟通建立了良好的关系，他也“了解”并信任我。

经过一番讨论之后我们达成了共识，他起身回到西部，而17岁的我作为二房东帮他管理30套复式公寓。我还可以继续唠叨这个故事的细节，但我想重点已经充分表达了。（这个工作很棒，直到后来他要我帮他把物业卖掉。我及时完成了这最后的任务，这份工作也就告一段落。）

重点是我在没有任何恶意的情况下，构建了与他人的良好信任关系。我用几个月的时间与他沟通，在他的意识里构建了善良、有激情并且聪明的形象。在时机来临的时候，虽然想法荒谬，但是前期的铺垫使得这一想法能够被接受。

在重新回顾这段往事时，我有了新的认识。我当时并没有意识到这件事情当中的很多促成因素。从社会工程的角度看，铺垫工作包括在开始之前知道自己的目标。这个案例中，我并不知道最终会得到这一近似疯狂的工作，但是铺垫工作仍然起到了作用。

大部分社会工程案例的进程会更快，但我认为原则是相同的。即使是天才也必须遵守类似的原则。因为铺垫工作涉及个人的情感和意识，所以不要给他们怀疑的理由。所提的问题必须与你伪装的角色相匹配。要想准备工作奏效，之后提出的问题要与你前期植入的意识相匹配。例如，如果我的建议是到客户的家乡并给他带回一些拍摄的相片，而不是为他管理物业，就和他对我的认识不相匹配，因为我的形象是一个灵活、有生意头脑及有爱心的年轻人。最后，在目标达成时，必须对客户有益，至少让他认为有益。在我的例子中，客户能够感觉到的好处是充分的。但是在社会工程中，可能只是一些“吹嘘”，为他人提供一个夸口的平台，或者提供一些更加实在的好处，包括身体、金钱或者心理上的好处。

练习诱导，不断变得熟练，你就会变成杰出的社会工程人员。从逻辑上来讲，下一节将介绍怎样成为一个成功的诱导者。

### 3.2.2 成为成功的诱导者

通过分析我个人的经历，我可以总结出自己从5岁起直到现在取得成功的关键要素。

- 不惧与他人交谈，并处于非“常规”场景中。
- 真心关心他人，即使是陌生人。乐于并享受倾听。
- 只在有了真正的解决方案时才提供建议或帮助。
- 在他人说出自己的问题时，不做主观判断。

确实存在成功诱导的关键元素。美国国土安全部有一个供内部员工使用的有关诱导的小册子，我有幸拿到并放在了www.social-engineer.org/wiki/archives/BlogPosts/ocso-elicitation-brochure.pdf上。

这本小册子中有一些十分精彩的观点。基本上，按照小册子及本章中的描述，诱导的应用在于其有效性、很难察觉及不具威胁性。该手册采用了“怎样避免”的角度来描述诱导，但是其后续章节给定了一些场景以展示其要点。

#### 1. 唤醒他人的自我

美国国土安全部的手册中的场景如下。

**攻击者：**“你的工作一定很重要，某某认为你很厉害。”

**目标：**“谢谢，谬赞了，但是我的工作并不那么重要，也就是……”

唤醒他人自我的方式简单有效，但是要注意如果滥用这一强大的工具，或者不是出自真心，则会让目标失去热情。你不会到处和人说：“哇噢，你真是全球最重要的人，长得还那么帅。”这样说只会引起别人的警觉。

唤醒他人的自我需要微妙的处理。如果你碰到的是一个真正的自我陶醉者，在听他夸耀过往成就时，眼珠不要转，不要叹气，也不要争论。微妙的自我唤醒要像这样，“你的那个研究改变了很多人在……方面的观点”或者“我无意中听到史密斯先生在那边说，你是他最敏锐的数据分析师”。要达到目的，但不能说得太明显。

据美国国土安全部的手册介绍，精心的吹捧会促使他人说出一些从未透露过的信息，而这正是社会工程人员想要的结果。

#### 2. 表达共同的兴趣

考虑如下的模拟场景。

**攻击者：**“哇噢，你有ISO 9001规范数据库的背景？那么你该看看我们开发的辅助认证的报告引擎模型，我可以发给你一个副本。”

**目标：**“太好了。我们正琢磨着在系统中添加一个报告引擎呢。”

表达共同兴趣是诱导的一个重要方面。在上面的特殊情境里，甚至比“唤醒自我”更加有效，因为它迅速拓展了关系，超越了初始交流范畴。目标同意进一步接触，同意接收攻击者发送的软件，且表达了以后继续讨论公司软件计划的兴趣。所有这些都会导致大规模安全入侵。

此时的危险在于攻击者完全掌控了形势。他控制了下面的步骤，发送什么信息、多少信息以及何时发送。对社会工程人员来说，这一步相当有利。当然，如果是长期目标，可以找一个能共享的软件，那就更有利了。共享有用的、非恶意软件能够构建信任及和谐的关系，使目标产生进一步交流的责任感。

#### 3. 故意说错

不经意间说错一些事情似乎会适得其反，但处理得好的话却是一件利器。

**攻击者：**“所有人都知道XYZ公司这方面的软件销售得最多。”

**目标：**“事实可不是这样。我们公司从1998年就开始销售类似的产品，通常我们的销售记录超过他们23%以上。”

有效使用这种表达方式会诱导目标说出真实的数据。大部人在听到错误表述时会有校正的欲望，似乎他们的正确性受到了挑战。告诉他人、显示自己的博闻强识、不能容忍错误表达等欲望

似乎是人类的天性。充分理解这一点，可以让这一场景变得很强大。你可以通过这种方式让目标说出事实的全部细节，也能在一群人中立刻发现谁对这一主题最为了解。

#### 4. 主动提供信息

美国国土安全部的手册中对人的共性做了很好的概括。本书前面提到了一些，后面会有更详细的介绍，其中*责任感*就是一种很强大的力量。作为社会工程人员，在交流中主动提供信息会迫使目标提供具有同样价值的信息。

想要试一下吗？下次在和朋友聊天时这样说："听说露丝的事了吗？我听说她被辞退了，而且现在找工作也很困难。"

大部分时候你得到的反馈是："啊！没听说呢。真不幸。我听说乔在办离婚，好像房子也保不住了。"

人类具有同情心，倾向于"同病相怜"，该示例就把这一点体现得淋漓尽致。人们喜欢分享类似的新闻。社会工程人员可以利用这一倾向，为谈话设定基调或氛围，从而构建出责任感。

#### 5. 假装高深

另一个强大的操纵工具就是*假装高深*。一般情况下，如果对方具有某一方面的知识，和他讨论相关问题并无不当。攻击者可以审慎地利用这一点，首先展示一些信息，假装知道一些内情，然后使用诱导技术展开话题。过程中可以把别人的观点当成自己的说出来，进一步强化自己的专家假象。下面的例子可以很好地说明这一点。

有一次，我要到A国商谈一笔大宗原材料交易。会谈需要我对目标公司具有详细的了解，而且必须要在见到他们之前做到这一点。之前我们从没见过，所以在谈判之前我去参加了一个在A国举办的会议。会议中我恰好听到了一个对话，讨论的是在和A国人的谈判中如何占上风。

我知道这是一次机会，而且更妙的是谈话小组中的一个人正是来自我要会面的公司。我快速加入其中，并且知道如果我不能快速地表达观点就会显得很尴尬。我这方面的知识不足，但是不必让他们知道。在他们谈话的间隙，我开始谈论"关系"理论。关系就是两个人（可能来自不同的社会阶层）如何产生联系，之后一人迫于压力为另一个人提供帮助。我谈到了怎样使用这种联系，总结中还提到：作为一个美国人，不能仅将名片塞进裤子后面的口袋里，而应该仔细研究、添加备注并将它们放在恰当的地方。

这番发言足以显示我的学问，让我有资格被列入值得信赖的人之列。表达过自己的观点后，我坐下来听其他人讲述自己的经验以及他们和A国大公司谈判方面的个人心得。目标公司的那位先生开始发言时，我更是极度关注。我敢肯定他发言中所表达的"观点"与其公司的经营理念紧密相关。这项收获比我能买到的信息都要有价值得多，也使得我后来的A国之行得以圆满成功。

还有一些诱导中常用的场景。

#### 6. 利用酒精的影响

在挖掘秘密方面没有比酒精更有效的东西，这一点很悲哀，但却是事实。如果在上述5个场景中加入酒精元素，则效果会放大10倍。

也许最好的方式就是以真实的故事来阐明。

1980年，洛斯阿拉莫斯实验室的一位资深科学家访问B国的一个研究院，举办一个关于他的专业——核聚变的讲座。他在核武器方面具有丰富的知识，但他知道这方面是禁区，所以需要将讲座的内容限定于他的研究主题。

过程中，有很多问题与核武器直接相关，且问得越来越细。攻击者的战术也会改变，他们也会问一些有关聚变和天体物理方面的问题。

在为他庆祝的鸡尾酒会上，人们不断走上前，赞扬他的学识和研究，每次都要祝酒和干杯。逐渐地，人们开始问一些绝密问题，例如氘和氚的点火要求，这两种元素都是中子弹的组成部分。他对这些问题防护得很好，但是在喝多了之后，他决定给出一个类比。他于是说，如果将这两种元素混合成一个球从桌子上滚下来，它们就可能点燃，因为它们的燃点都很低。

这个看似无用的信息可能为B国的核武器研究者提供了清晰的指引。他们会与另一位科学家交流，然后得到更多的知识，以此类推，逐渐获得越来越多的知识。在很多尝试之后，B国的科学家终于掌握了清晰的蓝图。

这是一个利用诱导术逐步获取整个答案的真实案例。你也可以在社会工程活动中采用诱导术。所有的答案并非来自同一个地方。你可能从某人口中得知有关日期和地点的信息，然后使用这一信息从他人口中诱导出更多的信息，以此不断深入，直到得到全部的信息。如何将这些信息聚合在一起，这是其中最困难的部分，需要完美的诱导技巧，这会在后面讨论。

### 3.2.3　提问的学问

作为社会工程人员，你必须认识到，诱导的目的不是走过去问：“你们服务器的密码是什么？”

你的目的是得到一些看似无用的琐碎信息，然后使用它们构建出你所寻求的答案的全貌，或者通过它们一步步取得答案。不管使用何种方式，这类信息收集方式都会为社交人员达成目标指明清晰的方向。

如何知道使用何种类型的问题？

下面将分析存在的几类问题以及社会工程人员如何使用它们。

#### 1. 开放式问题

开放式问题不能仅仅用“是”或“否”来回答。如果是问“今天外面相当冷啊，是吧？”，

得到的只能是“是啊”、“啊”、“嗯”之类的答案。如果你的问题是“你觉得今天的天气如何？”，那么引出的就是有效的回应，而不仅仅是“是”或“否”。

社会工程人员可以通过分析和研究优秀的记者来学习如何使用开放式问题。优秀的记者必须使用开放式问题，以持续诱导被采访对象回答设定的问题。

设想我约了朋友会面，但是他取消了这次活动，我想知道具体原因。我的问题会是这样的：“你取消了前几天的会面计划。到底是怎么回事啊？”

“我感觉不太舒服。”

“哦，希望你现在好点了。什么地方不舒服？”

通过这一连串的问题通常会得到更多的信息。如果仅仅是责备的话，效果就不一定了，比如问道：“伙计，到底是咋回事啊？那天你竟然放我鸽子！”

开放式问题的另一个强大之处是多使用*为什么*和*怎样*。如果问题中包含*为什么*或者*怎样*，就会得到对原始问题的深入解释。

这些问题都不是通过“是”或“否”就能回答清楚的，对方会暴露一些你感兴趣的细节。

有些人会抵触开放式问题，所以使用*金字塔方法*会好一些。先从范围较窄的问题开始询问，随着谈话的进行会聊到更宽泛的问题。如果你真想用好这一技术，可以从询问青少年开始训练。

例如，很多时候开放式问题会是这样的：“今天上学怎么样啊？”得到的回答会是：“还行。”再无他言。这样的回答没有任何意义，所以问一些范围较窄的问题会得到更多的信息。

“今年你们数学教什么？”这个问题的范围很窄，只能用特定的回答：“代数II。”

“啊，我很讨厌代数。你喜欢吗？”

从这里开始，可以拓展到更宽泛的问题，而且一旦使目标打开了话匣子，获取信息就变得容易多了。

#### 2. 封闭式问题

显然，封闭式问题正好和开放式问题相反，但也是一种有效引导目标的方式。封闭式问题经常会限制回答的范围，通过不超过两种可能。

使用开放式提问，问题可能是：“你和经理的关系如何？”但封闭式问题就会是：“你和经理的关系好吗？”

封闭式问题的目的通常不会是要得到详细信息，而是要对目标进行引导。

司法人员和律师经常运用这种类型的推理。如果想要目标遵循特定的回答路径，他们的问题经常是封闭式的，不允许答案出现天马行空的可能。常见的询问方式如下。

“你认识被告史密斯先生吗？”

“是的，我认识。”

“6月14日夜晚，你在ABC酒店看到史密斯先生了吗？”

“看到了。”

“当时是什么时间？”

“晚上11点45分。”

所有这些问题都是封闭式的，应答只有一到两种可能。

### 3. 引导性问题

引导性问题结合了开放式问题和封闭式问题的特性，是具有答案暗示的开放式问题。例如，“6月14日晚上11点45分左右，你和史密斯先生在一起在ABC酒店，是吗？”。这种类型的问题会引导对方，并且为其提供表达自己观点的机会，但是其发挥的空间很狭窄。同时引导性问题暗示目标你对问题的答案已经有所了解。

引导性问题的答案经常为“是”或“否”，但是与封闭式问题有所不同，因为问题中植入了更多的信息，所以社会工程人员也能从中得到更多的信息。引导性问题陈述了部分事实，然后询问目标是否同意。

1932年，英国心理学家弗雷德里克·巴特莱特（Frederic C. Bartlett）总结了记忆重构的研究结果。他告诉实验对象一个故事，然后让他们立即回忆其中的事实，两周以后以及四周以后再次进行回忆。巴特莱特发现，实验对象根据他们的文化背景、信仰和个性修改了故事，没有人可以正确地回忆出完整的故事。这证明了记忆并非是对过去的正确记录。似乎人们会构造记忆来契合自己对世界的已有认知。在被询问时，很多情况下，我们的记忆库是基于自己的感知和对自己重要的事情而形成的。

正是因为这样，通过引导性问题来操纵人们的记忆是可行的。伊丽莎白·洛夫特斯（Elizabeth Loftus）是一位目击者证词研究领域的开拓者，她演示了通过使用引导性问题扭曲人们对某事的记忆是极有可能的。例如，如果你给他人看一张没有放泰迪熊的孩子房间的照片，然后问他：“你有没有看到一个泰迪熊？”你并没有暗示他房间里有一个泰迪熊，所以他会按照自己的想法回答“有”或“没有”。然而，如果问题是“你看到泰迪熊了吗？”，这就暗示了房间中有泰迪熊，通常人们的答案会是“看到了”，因为泰迪熊与人们对孩子房间的认识具有相关性。

这些研究表明，引导性问题是专业社会工程人员手中的一件利器。学习怎样引导目标也会增强社会工程人员收集信息的能力。

4. 假设性问题

假设性问题就是其字面的含义——你会假设对象已经拥有特定的知识。通过假设性问题，社会工程人员能够确定目标是否拥有他想要的信息。

例如，司法人员采用的一门技巧就是假设目标了解某些事（如了解某人），于是会问："史密斯先生住在哪里？"根据问题的答案，该司法人员可以确定目标是否认识对方及其熟悉程度。

社会工程人员在使用假设性问题时，有一点需要注意，即不要让目标了解事情的全貌。如果目标了解了整个意图，社会工程人员会丧失对环境的部分控制能力，控制权会反转。社会工程人员也不能通过假设性问题指责目标的失误，这样会疏远目标，同样导致自己丧失控制权。

在使用假设性问题时，社会工程人员最好已经对事实有所了解，然后将事实贯穿在问题中。如果假设性问题中携带了虚假信息，只会让目标失去兴趣，得到的结果只能是目标不知道某些不曾发生的事情。回到前面的例子，为了从一位重要的化学专家那里获取信息，我做了一些前期研究并学到了足够的知识，也许可以问出一个精妙的假设性问题，但是如果我不能满足目标对我知识的预期，则会将整件事搞砸。

举个例子，假设我的问题是："因为氘和氚的温度阈值都很低，在处理它们的时候怎样避免燃烧呢？"如果我不是核物理学家，可能很难理解后续的内容，这样会适得其反而且没什么用处。要对假设性问题进行规划才能取得最大的效果。

在询问假设性问题时，司法人员掌握的一件有用的法宝就是："在回答下一个问题之前，请考虑清楚……"这句话给对方的暗示就是在回答问题时一定要诚实。

掌握这些技巧需要成年累月的训练。如果前几次尝试不成功也不要沮丧，要不断尝试。不要有畏惧，下面有掌握这一技巧的窍门。最后还会有一个综述。

## 3.3　精通诱导

本章有很多信息需要消化吸收，如果你不是那种善于和人打交道的人，使用本章的技术会很艰难。与社交工程的大多数要素一样，诱导在应用中有一系列的原则，能够强化个人的沟通技巧。为帮助你掌握这些原则，请记住以下几点。

- 问题太多会吓跑目标。用一堆问题轰炸目标不会有任何收获，只会让对方害怕。记住，对

话是一种有来有往的交互，你想要问，但也要告诉对方一些信息，让对方感到自然。

- 问题太少会让对方不自在。你曾经碰到过“尴尬沉默”的场景吗？这样不会有效果，对吧？不要假设目标善于交谈，会长篇大论、滔滔不绝。你必须研究谈论的问题，让对话有趣。
- 一次只问一个问题。第5章会涉及思维缓冲区溢出，但是在这里你的目的不是使对方溢出，而只是收集信息，构建答案的轮廓。不能显得太急切，也不能兴味索然。

根据已收集的信息，要使诱导正常发挥作用需要微妙的平衡。信息太多、太少、太急切及不充分都会导致失败。

不过，这些原则有助于你掌握这一惊人的才能。不管是将该方法用于社交工程中，还是用于学习社会交往的技巧，都应遵循如下方法：将谈话想象成一个漏斗，上面是最大的、最“中性”的部分，底部是最窄的、最直接的部分。

开始时问一些相对中性的问题，通过这些问题收集一些情报。在对话中要你来我往，然后问一些开放式问题。如有需要，使用几个封闭式问题引导目标到我们感兴趣的部分。如果情况允许，进入漏斗底部，询问那些最直接的问题。从这个漏斗中流出的就是源源不断的有价值的信息。

考虑前面讨论的商业聚会酒吧中的情况，我的目标是获取情报，然后发起一次安全入侵。

交谈开始时我的问题是很中性的。“想清静片刻？”这个问题打破了对话的坚冰，通过其中的幽默元素为双方建立了平等沟通的桥梁。我又问了几个中性的问题，在问他的工作时呈上了自己的名片，这样对话持续平稳地进入了开放式问题环节。

经过前面简短的信息收集环节，可见谨慎地使用预设的封闭式或假设性问题是关键。当得知公司最近购买了新的财务软件且网络也升级了之后，我需要的就是以此为切入点且完成任务。通过对大楼安全措施的了解，我知道使用的是RFID，但不是很确定目标会进一步说明门卡的样式，并拿给我看。

这里就要应用直接的问题，即明确地询问公司使用的安全方式。在我使用这类问题时，我们的关系和信任程度已经达到很高的级别，他可能回答我提出的任何问题。

懂得如何与他人沟通是诱导者必须具备的技巧。社会工程人员必须适应并且能融入任何环境及情况下的交流。迅速建立与目标的初步信任是关键步骤，没有友好的关系，交流极有可能以失败告终。

其他的重要因素包括确保你使用的沟通形式、询问的问题以及说话的方式与自身的伪装相匹配。虽然知晓如何问出一个目标必须回答的问题是成功诱导的关键，但是如果所有的技巧和问题与你的伪装不匹配，则诱导也会失败。

## 3.4　小结

本章涵盖了全书最强有力的一些观点。之所以说“强有力”，是因为诱导技巧不仅会提升社会工程能力，也能提高沟通的水平。明白如何通过正确的节奏和方式问出恰当的问题，可以得到很多机会。作为社会工程人员，这是成败的分水岭。第一印象往往取决于外表，但是从你嘴里说出的话更是成败的关键。精通诱导技巧几乎可确保社会工程人员的成功，也会为你所扮演的角色大大加分。

本章也提到了伪装的强大之处。这是每个社会工程人员都需要关注的另一课题，无论是恶意的社会工程人员，还是专业的社会工程人员，都必须掌握。但是怎样确保实现这一目标呢？要回答这个问题，必须学习和理解何为伪装，详见第4章。

# 第 4 章 伪装：如何成为任何人

诚信是建立关系的关键。如果善于伪装，也能成功。
——理查德·杰尼（Richard Jeni）

有时我们会希望自己变身为另外一个人。我就常常很见鬼地希望自己能稍微瘦一点，帅一点。即使医学界还没有研发出一种快速变身的药物，但是解决这种窘境的方法确实存在，那就是伪装。

什么是伪装？有的人认为只是社会工程过程中编造的故事或者谎言，但是该定义是非常狭义的。更为精确的定义是，以背景故事、衣着、仪表、个性和态度来塑造角色以完成社会工程审计工作。伪装包括你所能想到的基于对象角色的方方面面。作为社会工程人员，你伪装得越全面就越令人信服。一般情况下，伪装得越简单，说明技术越娴熟。

伪装，尤其是从互联网出现以来，越来越多地被恶意利用。我曾经看到过一件T恤上写着："互联网上，男人是男人，女人是男人，小孩子是等待着你的FBI探员。"虽然这是句调侃，但这种说法有一定的道理。在互联网上，你可以随心所欲地装扮成任何人。这种伪装技术多年来一直被恶意黑客用来攫取利益，而且不仅限于互联网。

在社会工程过程中，角色扮演或者假扮别人以达到目的有时是必要的。克里斯·海德纳吉或许没有一个技术支持人员或者一个进出口公司首席执行官那么大的影响力。当一个社会工程情形出现，有能力成为那个要伪装成的人是非常重要的。在一次讨论会中，我和世界知名的社会工程人员克里斯·尼克尔森（Chris Nickerson）聊到这个话题，他说到了一些我认为真正切中要害的观点。

尼克尔森说伪装不是扮演某个角色或者出演部分剧情，不是撒谎后不停地圆谎，而是真的成

为那个人。你的一丝一毫都是正在扮演的那个人。走路的方式、说话的方式、肢体语言都与那个人一样。我同意他的这个伪装哲学。一部令人感到绝无仅有的电影，往往是因为演员的出色表演，他们对于角色巧妙、精准的演绎让我们难分真假。

这在我的生活经历中得到过验证，很多年前我和妻子观看了布拉德·皮特出演的精彩影片《燃情岁月》。电影中他扮演一个自私的混蛋，拥有一个饱受折磨的灵魂，做了很多错误的决定。他的表演如此到位，以至于我妻子讨厌了这个演员好几年。他就是个很好的伪装者。

很多社会工程人员以为伪装仅仅是乔装打扮。衣着的确能起到作用，但伪装是门学问。通过伪装这种表演方式，可以整个变成另外一个人。要实现这一点，社会工程人员必须明确到底什么是伪装，作出计划，并演绎完美的伪装，这样才有可能成功。本章将涵盖伪装的各个方面。首先会讨论伪装的确切定义。接着讨论作为一名社会工程人员如何去伪装。最后，会把这些结合起来，通过几则故事去展现如何有效地应用伪装。

## 4.1 什么是伪装

伪装的定义是创造虚构的场景以劝说目标受害者泄露信息或者作出某种行为。这绝不仅仅是说谎那么简单，在某些案例中有可能是创造一个全新的身份，然后用这个身份去获取信息。社会工程人员可以利用伪装技术扮演从事某些特定工作的人和他们从未担任过的角色。伪装没有固定的万能模式，社会工程人员必须在“职业生涯”中创造很多不同的伪装。所有伪装都有一个共同的特点：研究。娴熟的信息收集技术是伪装成功的关键。打个比方，如果目标不需要外部技术支持，即使我们将技术支持人员模仿得再完美也无济于事。

伪装不仅可用于社会工程中，也能在生活领域发挥作用。销售人员、公共演讲者、算命者、神经语言程序学专家，甚至是医生、律师及临床医学家等，都需要使用一定形式的伪装。他们都需要创造一个适宜人们泄露隐私信息的场景。社会工程人员和其他伪装使用者的差异在于目标的设定。社会工程人员必须完全变身为伪装的角色，而不仅仅是装腔作势。

只要审计或者社会工程没有结束，都应该继续伪装。我就进入过角色，我的同事也是，有人在事情过后还沉浸在扮演的角色中。无论去什么地方，都要是所扮演的角色。此外，很多专业社会工程人员具有多个在线身份、社交网站的身份、电子邮件和其他账户，可供伪装的时候用。

在我参与的社会工程播客节目中，曾经就该话题采访过电台明星汤姆·米施克（Tom Mischke），详细信息参见www.social-engineer.org/episode-002-pretexting-not-just-for-social-engineers/。电台主持人必须精于伪装，因为他们只能透露宜于发布给公众的信息。汤姆在这方面很在行，绝大多数的听众都认为自己“了解”他，像朋友一样。他被邀请去参加婚礼、纪念日甚至是生日聚会。汤姆是如何完成如此神奇的伪装的呢？

答案就是不断练习。他给自己安排了很多很多的练习。他告诉我，他会制定出“表演对象”并且勤加练习——使用他们的发声方式，像他们一样坐立，甚至学习他们的穿着。好的伪装只能源于不断的练习。

要记住非常重要的一点：伪装的质量与所收集的信息质量有直接关系。信息越多，信息的质量和相关性越高，越利于我们的伪装，也就越容易成功。比如，如果一家公司只使用内部技术，或者将技术外包给一两个员工的小企业，那么经典的技术支持人员伪装就会完全失败。当别人质疑你的真实身份时，尽可能表现得自然，这直接取决于你对伪装是否能够运用自如。

现在你已经了解如何利用这项技能了。下面介绍伪装的原则以及如何应用这些原则来计划出令人信服的伪装。

## 4.2　伪装的原则和计划阶段

像其他技术一样，伪装也有一定的原则可以遵循。下面列出了一些原则。当然，并不是说就只有这些，还可以继续添加，只是这些原则体现了伪装的本质。

- 调查越充分，成功的几率越大。
- 植入个人爱好会提高成功率。
- 练习方言或者表达方式。
- 很多时候，如果低估了电话的作用，可能会减少社会工程上的投入程度。不过对社会工程人员来说，使用电话并不会减少精力的投入。
- 伪装越简单，成功率越高。
- 伪装必须要很自然。
- 为目标提供逻辑结论或下一步安排。

下面各小节将详细讨论每一条原则。

### 4.2.1　调查越充分，成功的几率越大

这个原则不言自明，但还是值得多次强调，因为收到的成效直接和调查的广度与深度相关。正如第2章里讨论的那样，这是社会工程成功的关键。社会工程人员掌握的信息越多，实现有效伪装的机会就越大。还记得第2章中讲述的我的导师马蒂・阿哈罗尼的故事吗？他是如何说服一位高管访问他的集邮网站的？乍一看，对这家公司的进攻之路应该和金融、银行、融资或其他类似的事情有关，因为这是一家金融机构。马蒂做的调查越多，越觉得伪装成一个集邮册出售者最为合适。找出高管的兴趣所在，让马蒂可以轻易地入侵这家公司，而且确实奏效了。

有时候细节决定成败。记住，没有不相关的信息。收集信息时，寻找故事、物品或者个人的

特点也是很不错的主意。利用目标个人的性格或者情感依托可以使你离成功更近一步。如果社会工程人员发现首席财务官每年都向一个儿童癌症研究中心捐赠一笔资金，那么伪装时涉及一个与此有关的筹款活动极有可能奏效，尽管这听起来有点无情。

问题是恶意的社会工程人员会不假思索地利用人们的同情心进行伪装欺诈。在2001年9月11日纽约双子大楼被攻击之后，很多恶意黑客和社会工程人员利用人员伤亡为自己牟利，他们设立网站，发送邮件给目标的计算机，并成立虚假基金，利用人们的慈善之心骗钱。在2010年智利和海地发生地震之后，同样的事情再次发生，很多恶意社会工程人员建立网站，发布地震活动或者失踪人员的信息。这些站点利用恶意代码导致人们的电脑中毒。

这类活动在某个电影明星或者歌星死后会更加猖獗。搜索引擎优化和市场营销天才会在几小时内让搜索引擎将他们的文章置于首页。恶意的社会工程人员同营销天才一起建立含有对搜索引擎优化的恶意站点，提升搜索引擎排名，从而利用人们对搜索引擎的不断关注来吸引大家访问这些站点，他们就会获取信息或者传播病毒。

有人会利用他人的不幸来牟利，是这个世界的可悲事实，这就是我所说的本书涉及的黑暗角落之一。作为一名社会工程审计人员，我可以利用一个雇员的感情向对方公司展示，表面上的好意会让这名职员泄露公司宝贵的商业运作数据。

所有这些例子都明确地表达了一点，社会工程人员信息收集和调查过程执行得越好，他促进伪装成功的几率就越高。

### 4.2.2 植入个人爱好会提高成功率

通过个人爱好去提高社会工程的成功率听起来很天真，但是有助于让目标信服你。如果开始时宣称自己在某一方面很擅长，最终却显示出这方面知识的匮乏，这绝对是毁掉信任关系的最快方式。作为一名社会工程人员，如果你从没见过服务器机房，没有拆过电脑的话，伪装成一个技术人员是很容易失败的。伪装中加入自己感兴趣的话题和活动，从而能够侃侃而谈，会使你显得聪慧而自信。

自信有助于说服目标相信你就是你宣称的那个人。某些伪装（例如集邮爱好者和核弹研究人员）需要更多的知识以让他人信服，这里我们又不得不提起前期研究。有时候伪装则比较简单，只要看一些网站或者读一本书就足够了。

对于社会工程人员来说，获取知识、研究感兴趣的话题，这是非常重要的。在伪装时，你可以聊故事、观点和工作，也可以聊你很了解的某种兴趣爱好，或者是一些谈起来很舒服的话题，看看这些能否奏效。

汤姆·G. 史蒂文斯（Tom G. Stevens）博士说：“记住，你的自信心始终与任务和自身处境密切相关。不同情况下，我们的自信心是不一样的。”这种说法很正确，因为自信心直接跟

别人如何看待你这个社会工程人员有很大关系。自信（只要不是自大）可以建立信任和默契，而且让人感觉很放松。尽量让目标谈论你感到舒服的话题，然后你就可以自信地发挥，这点很重要。

1957年，心理学家利昂·费斯廷格（Leon Festinger）提出了认知失调理论。该理论认为，人们倾向于协调自己的信仰、观点乃至几乎所有的认知。如果态度和行为之间存在不协调，就必须要修正这种不协调。费斯廷格博士提出有两个因素会影响这种不协调的强度：

- 不协调的信念的数量
- 每个信念的重要性

随后他提出3种消除这种不协调的方法（每个社会工程人员都必须竖起耳朵听）：

- 降低不协调信念的重要性
- 增加更多的协调信念以超过那些不协调的信念
- 改变那些不协调的信念以使它们协调

社会工程人员如何利用这些信息呢？当伪装的角色需要你表现自信的时候，表现得不自信就会很自然地产生不协调。这些不协调引发各种红色警告，给你们之间的默契、互信和下一步进展带来障碍。这些障碍会影响目标人物的行为，他们会设法平衡自己不协调的感受，这样你的伪装就失败了。

避免这种情况发生的一种方法，是加入更多的协调信念以使其数量超过那些不协调的。目标对你的伪装角色有何期待呢？了解这些可以让你通过行动、谈吐和态度去迎合目标人物的思维和情感，从而建立起信念系统，让他们忽略任何值得怀疑的地方。

当然，一个技术娴熟的社会工程人员同样可以将不协调的信念变协调。虽然这很棘手，但是这项强大的技巧确实值得拥有。有可能你的伪装和目标的构想不一致。你可以回想一下《天才小医生》（*Doogie Howser, M.D*），豪斯医生很年轻，这和角色设定的顶级医生似乎不相符。这是个不协调的信念，但是他的渊博知识和行为又让“目标”认为这是协调的。就像之前的例子，社会工程人员可以通过观点、行动，尤其是知识，让他的伪装和目标的认知达成一致。

2010年举办的第18届Defcon峰会上，我见证了这样一个案例。我是社会工程夺旗竞赛（Capture the Flag，CTF）的组织者之一。我们发现很多选手伪装成内部雇员。当问到他们“你的工号是多少？”时，不成熟的社会工程人员会很紧张，要么回答不出要么直接放弃比赛，然而一个训练有素的社会工程人员却不会让目标产生任何不协调的想法。他会随口说出一个在网上找到的工号，或者用其他方法说服目标没必要提供工号信息，以此来消除目标的疑虑。

看似我们在以很专业的口吻解答非常简单的问题，然而，你必须得明白：伪装的方法虽多，但也是有限度的。请明智地选择适合你的那一种。

### 4.2.3 练习方言或者表达方式

学会用不同的方言与人沟通会给人留下深刻的印象。受居住地的限制，要学会说一种不同的方言或者口音需要一些时间。不是说不可能，只是学会像美国的南方人那样慢声细语地讲话或者学会亚洲人的口音会非常困难。有一次我参加一个国际营销组织举办的培训课程，他们提供的一些统计数据说明，70%的美国人更喜欢聆听一个英式发音的人讲话。我不确定这个统计数据是否属实，但是我会说我喜欢自己的口音。那个课程之后，我听说不少参加课程的人开始练习英式发音了，他们的发音真的很糟糕。我在英国有一个好朋友，名字叫乔恩，当他听到美国人试图去模仿英国口音来表演《欢乐满人间》时非常生气。如果他听到我们组说的英式发音，估计会气炸了。

这个课程让我明白，即便统计学告诉我们哪一种口音更利于销售使用，或者是因为你要到南方或者欧洲去做社会工程，这些都不意味着你可以轻易学会当地的口音。在存疑的时候，就扔到一旁。如果不能让你的方言完美、自然流畅，就不要去尝试。演员们为了和角色的口音一致并且发音清楚，需要专门的声乐教练及培训课程来练习发音。克里斯蒂安・贝尔（Christian Bale）是威尔士人，但是想从口音中辨别出来这点非常困难。在他大多数的电影里，他听起来并不像英国人。而电影《莎翁情史》中的格温妮丝・帕特洛（Gwyneth Paltrow）的英式口音就相当明显。

大多数的演员有方言教练帮助他们完善发音。因为大多数的社会工程人员请不起方言教练，所以可以看一些讲方言发音基础知识的书，比如伊万杰琳・玛琪琳（Evangeline Machlin）的《舞台方言》（*Dialects for the Stage*）。虽然这本书的出版时间比较早，但是包含了很多很棒的建议。

- 找到你想学的方言的例句听，像《舞台方言》这种书常常是附带录音带的，里面有多种方言。
- 努力跟着录音带说，学里面人的发音。
- 在感到自信以后，用该方言说话并录下，以便在事后听的时候纠正发音。
- 营造一个场景并和伙伴进行练习。
- 在公众场合用该方言说话，看看别人是否觉得可信。

世上有无数种方言和口音，我个人找到了一种很有用的方法，就是写下我要讲的话的音调。这样我可以练习朗读，并且记住大意，让我的口音更自然。

这些建议可以帮助社会工程人员掌握或者至少是熟练使用另一种方言。

即使不能掌握另一种方言，学会工作领域的专业表达方式也可以使情况有所改观。在公共场合听两个人交谈是一个好主意，餐厅、购物广场或者任何能找到一群人坐在一起聊天的地方都是绝佳的场所。仔细地听人们交谈所用的短语或关键词。当你听到他们在一些对话中运用的词汇时，可以考虑把它们纳入到你的伪装中，使其更可信。同样，这也需要研究和勤加练习。

### 4.2.4　使用电话不会减少社会工程人员投入的精力

最近几年，互联网开始主导某些“不需面对面交流”的社会工程活动。然而，在过去，电话是社会工程中不可或缺的一部分。由于这种转变，很多社会工程人员不再花时间和精力去探究“打电话”这件成功利器。

这里想说明的是，电话仍然是一种非常强大的社会工程工具，不该因为互联网的非人格化性质而减少对它的使用。

很多时候，社会工程人员在策划电话攻击时的想法会有所不同，因为利用互联网看起来更简单一些。要记住，在使用电话进行社会工程时，要投入同等的精力、同等深度的研究和信息搜集，最重要的是同等水平的练习。我曾和一个小组一起练习利用电话进行攻击。我们研究了适宜的方法、语调、语速、音调以及措辞，然后过了遍剧本（通常一分钟左右的时间），开始了一个会话。第一个人打了电话，连线到某个人，刚开始的几句话就搞得一团糟。在彻头彻尾的尴尬和恐惧中他挂掉了第一通电话。这给我们上了很好的一课：话筒另外一头的人根本不知道你想说什么，所以你不会真的“搞砸”。练习会话可以帮助你学会处理那些意料之外的事，而这通常是由你不慎改变剧本所造成的。

如果没有一组人陪着你训练或磨练这些技能，你必须得有创造力。试一试给家人或者朋友打电话，看看你能在多大程度上操控他们。另一种练习方法是给自己录音，就像在打电话一样，然后重放一遍看看听起来如何。

我个人认为使用剧本大纲是很重要的。这里有个设想：想象你不得不给电话公司或者另外一个机构打电话。理由是他们搞错了一笔账单或者服务有问题，所以你打电话过去抱怨。在你跟客服解释以后，告诉他你有多失望，有多生气。客服没有为你提供任何帮助，他说：“本公司承诺提供最好的服务。请问还有什么需要帮助的吗？”如果电话另一端的人稍微思考一下他的问题，就会知道这样问有多傻，对吧？这就是使用剧本而不是大纲所导致的问题。大纲允许你有“艺术创造的自由”，让你在对话里中灵活机动，不必担心下面必须要发生什么。

使用电话提高伪装的可信度，是得到目标认可最快的方法之一。电话允许社会工程人员去“哄骗”或者假冒几乎任何事。看看下面这个例子。如果我想假装是在一个忙碌的办公室里给你打电话，我可以到www.thrivingoffice.com下载一段音频。这个站点提供了一个录音叫“忙”，另外一个叫“很忙”。它们的创作者称：“这个CD很有用，它包含人们可在一家公司听到的所有声音，让人们立即相信这是真实的场景。简单、有效而且质量有保障！”

这个句子就蕴含着社会工程的真谛——充斥着人们想要听到的办公嘈杂声。你发现这个CD能够满足你的预期，而且相当可信（至少在满足目标的预期后，他会是这样认为的），从而能够自动得到信任。

此外，伪造电话号码欺骗要相对简单一些。像www.spoofcard.com提供的服务或者一些自制的方法，都可以帮助社会工程人员改变来电显示的电话号码，让目标认为你是从公司总部、白宫或者当地银行打过来的。利用这些服务可以伪造出世界上任何地方的电话号码。

电话对于社会工程人员来说是非常有用的，养成使用电话的习惯，给予它足够的尊重，可以增强社会工程人员伪装的技能。因为电话是如此有效的工具，而且它的效力还将持续下去，所以必须在它身上花费相当的时间和精力，让它在任何社会工程场景中发挥作用。

### 4.2.5 伪装越简单，成功率越高

“越简单越好”的原则一点也不夸张。如果伪装有很多错综复杂的细节，以致忘记任何一个都会导致失败，那么就真的会失败。保持故事情节、事实和细节的简单性，会增强可信性。

人际欺骗领域有名的心理学家和研究人员保罗·艾克曼（Paul Ekman）博士，在1993年发表了一篇联合署名的文章，名为“失败的谎言”（Lies That Fail）。在那篇文章中他认为：

> 很多时候你没有时间去准备故事情节、进行练习和记忆。就算事前有很充分的预案，也有可能突然冒出一个不能预见的方向，说谎者不可能聪明到可以预见所有可能被问及的问题，也不可能准备所有的答案。仅有聪明的头脑是不够的，环境中不可预见的变化会导致原先有效的准备变得不可行。而且，即使不是为情势所迫改变方向，某些撒谎者也会由于记忆问题想不起前面的描述，结果不能快速一致地解答新的问题。

这个重要观点将为什么越简单越好解释得很清楚。如果伪装很复杂，努力去记住伪装的全部内容基本是不可能的，一个很小的错误就可能把你的伪装全部毁掉。伪装应该尽可能地自然、顺畅，应该容易记住。如果觉得很自然，那么回忆之前的事实和故事就不会是负担。

为了表明细节记忆的重要性，我想跟大家分享一则小故事。我曾经从事过销售领域的工作，被安排和一位销售经理一起共事、学习。我还记得他给我上的第一堂课。我们开车到客户的家门口，在下车之前，他看了看信息卡，告诉我：“记住，贝姬·史密斯（Becky Smith）发过来一个请求卡，要求补充保险。我们要用XYZ策略。仔细观察，好好学。”

在前3分钟里他称她为贝斯或贝蒂，每次他叫错名字，我都看到她有情绪波动，然后她会很轻地说：“是贝姬。”尽管我们已经给了她很大的优惠，但依然被拒绝了。她对于自己的名字总被说错很失望，所以对于听到的任何东西都不感兴趣，也听不进去了。

这个场景真实体现了保持简单的重要性。

除了记住事实之外，不过分追求细枝末节也很重要。一个简单的伪装允许故事发展，并且允许目标运用想象去填满空隙。不要试图将伪装设计得很精致，只要记住那些伪装中比较关键的小细节即可。

此外，还有一个有趣的花招：知名罪犯和骗子的一个常用伎俩是故意犯一些错。这个想法是基于“人无完人”而建立的，一些错误会让人感觉很真实。如果运用这个策略，得留心选择决定去犯的错误，虽然这确实让对话看起来更自然，但它增加了伪装的复杂性。少用这一花招，如果一定要用，尽可能地简单。

现在我用以前审计过程中使用过或看见过的例子将上面几点结合起来。通过打电话的良好诱导，一名社会工程人员知道了公司所用的清洁公司的名字。通过网上搜索，他找到了能打印出来的清洁公司的标识。有很多本地或者网上商店可以按照客人的要求将标识印在衬衫或帽子上。

对照模板调整了几分钟，他订购了一件衬衫和一个球帽，上面印有垃圾回收公司的标识。几天过后，穿着印有标识的衣服，带着一个写字夹板，这位社会工程人员来到了目标公司的保安亭旁。

他说：“你好，我是ABC垃圾回收公司的乔，我们接到你们采购部门的电话，要求派一个人来检查后面被损坏的垃圾箱。明天会来人收垃圾，如果这个垃圾箱无法修复，我会让他们带一个新的来。但是我得去后面检查一下。”

保安人员毫不迟疑地说：“好吧，你需要带着这个徽章过去。经过这里再绕到后面，就可以看到垃圾箱了。”

社会工程人员顺利拿到了通行证，对垃圾箱进行了长时间仔细的翻查，但是他还想扩大战果，试图进一步发现线索。他看着写字板说：“这里显示说要检修的不是食品垃圾箱，而是装纸张和技术垃圾的。到底会在哪里呢？”

“哦，照着我告诉你的路线，它们在第3隔间。”保安说。

“谢谢！”乔说。

简单的伪装，穿着有标识的衣服，带着“工具”（如写字板），并且故事情节简单而又好记。正是它的简单性和缺少细节使得这次伪装更加令人信服，进而发挥作用。

另一种惯用的伪装就是所谓的技术支持人员。只需一件Polo衫、一条卡其裤与一个小的电脑工具包。许多社会工程人员使用这种技术顺利进入了公司大楼，因为“技术人员”通常能不受监督地进入任何地方。同样的法则也适用于这里，即保持故事情节的简单会使这种伪装真实可信。

### 4.2.6　伪装必须显得自然

想要使伪装看起来自然一些，可以采用我前面推荐的大纲模式，而不是使用剧本方式。大纲模式下社会工程人员可以自由地发挥，使用详细的剧本则会太机械。伪装中可以加入社会工程人员感兴趣的项目或故事。假如每次有人问一个问题或做出一个论述，你都支支吾吾，需要深入地思考，而不能做出及时明智的回答，可信性就会因此大打折扣。确实，很多人都是思考后再说，

因此这并不是要求你立即答复，但是要有答案或者要找到一个没法回答的借口。比方说，有一次对方在电话中询问一则我不知道的信息。我就说："让我找找。"然后我迅速看了一遍，假装我是在大声询问同事："吉尔，麻烦让比尔给我份XYZ账户的订货单。谢谢！"

然后"吉尔"会拿来表格，我就可以得到需要的数据，而表格再也不会被提起。

下面列出了几条让伪装更加自然的方法。

- **不要考虑自己的感受**。这点很重要，因为通常在伪装时如果想太多就会融入更多的个人情绪，然后恐惧、不安或焦虑就会随之而来，这些都可能会导致失败。另外，你可能不会经历不安或焦虑，但会过度兴奋，这同样会使你犯很多错误。
- **不要把事情太当真**。当然，在生活中这就是一条好建议，而且同样非常适用于社会工程学。作为一名专业的安全人员，你有一份很严肃的工作，这是一件严肃的事情。但是如果不能笑对自己的错误，就可能会沉默不语，或者在处理后续的小事情时如临大敌。当然，我并不是建议你视安全如儿戏。但是，如果你将潜在的失败当做人生中巨大的失败，那么产生的压力恰恰会导致最坏的结果。只有正确看待小的失败，才能取得更大的成功。
- **学会找到相关信息**。我喜欢用"摆脱思维的束缚，融入这个世界"来描述这个理念，这是一个非常棒的建议。社会工程人员可能全力计划好了前3个步骤，但却遗忘了一个可能会使伪装土崩瓦解的关键细节。要始终留意身边出现的信息和状况，包括目标的肢体语言、说的话，微表情（第5章会详细介绍）等，然后将其应用到自己的行动中。

  同时，记住说话者能看出什么时候你没在认真听他说话。这会让很多人感到不爽，就算是无关紧要的句子，没有被听取也会招致不快。每个人都经历过自己的话被人当做耳边风，或许他们有各自正当的理由开小差，但这样做真的挺让人扫兴的。

  一定要注意听目标所说的话。集中注意力，你会听到一些对他们很重要的细节，同时也能够获取有助于自身取得成功的信息。
- **争取多积累经验**。在这本书里，你可能会反复看到一个词语，那就是练习。通过实践积累经验，能成就伪装也能识破伪装。有意识地、毫无目的地在和家人、朋友甚至是陌生人的交往中练习自然地伪装。抛开死缠烂打的方式，与他人展开简短的会话，可以使你在伪装的时候表现得更加自然。

这些方法绝对能使社会工程人员在伪装时处于优势地位。具备自然伪装的能力是一种天赋。本章前面谈及了我对汤姆·米施克的采访，他对表现自然持一种很有趣的看法。他说他在练习和准备的过程中，都会将"表现自然"作为一个目标。每次伪装前，他都会进行大量的练习，以至于足以使伪装自然得像是幽默与天赋的产物。

### 4.2.7 为目标提供逻辑结论或下一步安排

无论你相信与否，事实是人们都希望被告知下一步该做什么。想象一下，你去看病，医生走

进来给你检查了一番，并且在记录纸上写了一些东西，然后说："好了，下个月见。"这是让人无法接受的。就算是听到坏消息，人们也希望被告知下一步该做什么。

作为一名社会工程人员，你要离开目标时，可能需要他采取或不采取行动，或者你已经得到想要的，只需离开。无论是什么情况，都应给目标一个结论或不会令其怀疑的下一步安排。

就像医生给你检查了身体，然后没有任何指示就打发你回家。如果在社会工程中，伪装成技术支持人员进入一幢大楼，在复制好数据库之后一句话也不说就离开，会让每个人产生疑惑：到底发生了什么事？甚至有人可能会给技术支持公司打电话，询问是否还要他做什么，或者最坏的情况是让他们自己胡乱猜测。无论是哪种情形，这种一句话也不留的离开方式都是有问题的。哪怕简单的一句"我已经检查了服务器并且修复了文件系统，你们会发现系统在未来几天里运行速度会提高22%"，都会让目标觉得"他们的钱花得值"。

令社会工程人员感到棘手的是让目标在他走后采取行动。如果这一行动对完成社会工程审计非常关键，你会想要自己主动出手。比如在第3章中，我讲到在一个商业会议活动中收集信息的案例，如果想让目标给我发邮件，我会说："这是我的名片，你是否可以在星期一给我发一封邮件，详细介绍一下XYZ公司？"他可能会记得给我发，也可能一回办公室就把我忘得一干二净了，这样整个事件会以失败告终。也许这样说会更好："我非常想从你那里了解更多的信息。在周一时我可以给你打电话或者发邮件询问更多细节吗？"

你提出的要求也应该和自己伪装的身份相匹配。如果你伪装成技术支持人员，则不应该"命令"周围的人必须做什么或者不能做什么，因为你在为他们提供服务。如果伪装成UPS快递员，你就不应该要求进入服务器机房。

正如之前提到的，一次完美的伪装还需要很多的步骤，但是对于需要进行完全可信的伪装的社会工程人员来说，本章的内容已经足以为你夯实基础了。

你可能会问："好吧，你列出来这么多原则，那接下来该如何呢？"社会工程人员要如何做，才能在电话里或者与他人面对面的交流中，进行前期调研充分、可信、语气从容而简单的伪装呢？怎样才能得到想要的结果呢？欲知详情，请继续阅读本书。

## 4.3　成功的伪装

要学习如何进行成功的伪装，就需要了解那些曾经成功伪装过的社会工程人员的故事，学习他们是如何展开伪装的。当然，他们的伪装最后都被识破了，因此我们现在才能读到这些故事。

### 4.3.1　案例 1：斯坦利・马克・瑞夫金

斯坦利・马克・瑞夫金（Stanley Mark Rifkin）一手策划了美国历史上最大的银行抢劫案（关

于他的相关信息，请参见www.social-engineer.org/wiki/archives/Hackers/hackers-Mark-Rifkin-Social-Engineer-furtherInfo.htm）。他是一名电脑极客，在他的小公寓里开了家电脑咨询公司，他的一个客户是给美国证券太平洋国民银行（Security Pacific National Bank）提供电脑服务的公司。坐落在洛杉矶的美国证券太平洋国民银行总部有55层，看上去就像一个用花岗岩和玻璃建成的堡垒。着深色制服的保安在大厅里巡查，隐藏的摄像机记录着每个来银行办理存取款业务的客户的一举一动。

这幢大楼看起来无懈可击，那么瑞夫金是如何在不携带任何武器、不动一分钱、不胁持任何人质的情况下带走1020万美元呢？

银行的电汇机制应该是很安全的，每笔电汇都必须输入密码，而且这个密码每天都会被强制修改，只有特定的人知道。密码被贴在安全房间的墙壁上，而且只有"特许人员"才可以进入这个房间。

前面提到的存档文件中是这样记录的。

> 1978年10月，瑞夫金来到了美国证券太平洋国民银行，银行工作人员理所当然地认为他是计算机工作人员。他坐电梯来到电汇室所在的D层。伪装成友好而且和蔼可亲的年轻人，他竟然进到墙上贴有当天密码的那个房间里。瑞夫金记住了密码，然后在没有引起任何怀疑的情况下离开了。
>
> 很快，银行电汇室的员工接到了迈克·汉森（Mike Hansen）打来的电话，他自称是该银行国际分部的员工。他正确地给出了当天的密码，要求为纽约欧文信托公司资金账户进行常规转账。整个过程没有任何引起怀疑的地方，所以美国证券太平洋国民银行就把钱打到了纽约银行的账户上。银行官员不知道的是，那个自称是迈克·汉森的男人其实是瑞夫金，他通过银行的安全密码盗取了1020万美元。

这个案件留下了许多可圈可点之处，但是现在我们把焦点集中到伪装上面来，仔细想想瑞夫金作案的细节。

- 为了能够在密码房间里不引起怀疑，他需要足够的自信和镇定。
- 提出汇款要求，他需要编一个足够令人信服的故事，而且需要考虑足够多的细节来自圆其说。
- 面对可能出现的问题，他要表现得足够自然。
- 为了不引起银行员工的怀疑，他说话要足够熟练和流利。

这些伪装必须经过细致的安排，考虑到每一个极其微小的细节。直到遇见了一个前同事，瑞夫金才被揭穿。瑞夫金被抓的时候，认识他的人都非常吃惊，甚至有人说："他不可能是个小偷，人人都喜欢马克！"

很显然，他的伪装是很到位的。他的计划经过深思熟虑，安排周详，排练纯熟。他知道去那里的目的，并且每一步都做得很完美。站在陌生人面前时，他知道如何伪装。如果不是熟知瑞夫

金的同事看了新闻后把他指认了出来，他是不会被发现的。

更加令人吃惊的是，当瑞夫金被保释在外的时候，他又打算用相同的方法“抢劫”另一家银行，但是他的行为落入了政府侦查员设计的陷阱，他被抓住了，并且等待他的是8年的牢狱之灾。尽管马克是一个“坏人”，但是从他的故事中我们能够学到很多关于伪装的知识。他的伪装非常简单，完全是用他熟悉的事情来打造精彩的故事情节。

马克的计划是把偷出来的钱变成不可追溯的钻石。为了实现这一目标，他首先需要成为一名银行雇员以拿到钱，然后变成一个钻石收购商将这些现金“洗掉”，最后通过把钻石卖掉，获得可以使用的、无迹可寻的、干净的现金。

他的伪装不涉及装扮和说话方式的变化，却要依次扮演银行工作人员、钻石采购商和钻石销售商。这其中要完成3次、4次甚至5次的身份变化。他做得非常好，基本上欺骗了所有人。

马克知道他的目标是哪些人，并且按照我们前面提到的所有规则来一步步实现他的计划。当然，他的行为是不可宽恕的，但是他的伪装天赋却是令人羡慕的。如果把天赋用到恰当的地方，他很可能会成为一位伟大的公众人物、销售员或者演员。

### 4.3.2　案例 2：惠普

2006年，《新闻周刊》发表了一篇非常有趣的文章（详见www.social-engineer.org/resources/book/HP_pretext.htm）。故事基本上是这样的：惠普公司的董事长帕特里夏·邓恩（Patricia Dunn）女士雇用了一个专业的安全团队，这个团队又雇用了私家侦探，私家侦探利用“伪装”技术获取了通话记录。这些聘来的专业人士实际上伪装成了惠普的董事会成员及新闻记者。这一切都是为了找出惠普队伍中可能的泄密者。

邓恩女士希望获得董事会成员和一些新闻记者的通话记录（不是惠普公司内部的电话记录，而是这些人家中或者手机的通话记录），来查证她认为可能的泄密者。《新闻周刊》是这样写的：

> 5月18日，在加州帕洛阿尔托的惠普总部，邓恩在董事会上扔出了她的炸弹：她已经找到了泄密者！据在场的惠普董事汤姆·珀金斯（Tom Perkins）透露，邓恩展示了监视方案并且指出了那个董事，该人承认他就是CNET的泄密者。那名董事的身份至今还没有向外界透露。他道了歉，但之后对其他董事说：“我原本打算告诉你们所有的事情，为什么你们没有问过我呢？”珀金斯说，随后那名董事被请出了董事会议室。
>
> 这个事件中值得注意的是那个被称为“伪装”的话题。
>
> 惠普的这一事件还将公众的注意力吸引到了安全顾问为获得个人信息所采用的不合理的手段上。在外部顾问团发给珀金斯的一封内部邮件中，惠普承认他们通过有争议的“伪装”技术，获得了将那个泄密者和CNET联系在一起的书面记录。《新闻周刊》获

> 得了这封内部邮件的内容。美国联邦贸易委员会（FTC）认为这个技术涉及使用“欺骗手段”来获得他人的非公开信息：通话记录、银行卡和信用卡账号以及社会保险号等。
>
> 就拿案例中的电话公司来说，通常情况下伪装者会将自己伪装成客户，因为这些公司很少需要你提供密码，伪装者仅仅需要一个家庭住址、账号和诚恳的请求便能获取账号的详情。FTC的网站披露，伪装者会将这些信息卖给持证的私家侦探、金融贷款者、潜在的诉讼当事人以及对配偶有疑心的人，甚至卖给那些试图窃取资产或者骗取信贷的个人。FTC声明，伪装“是违法的”。FTC和若干州的检察长已就涉嫌违反联邦法和各州法律的欺诈、失实陈述及不公平竞争等行为对伪装者进行指控。惠普公司的董事之一，威瑞森（Verizon）公司的总裁拉里·巴比奥（Larry Babbio）已经以书面形式提交了打击伪装者的各种措施。

（如果你对具体内容感兴趣，可以在下面的链接中找到2006年的《电话记录隐私权保护法》：http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h4709enr.txt.pdf。）

最终的结果是刑事控诉不仅针对邓恩女士一人，她所聘请的顾问也被指控。你也许会疑惑：“怎么可能对他们进行指控呢？他们是签了合同、被雇用来进行这些测试的啊。”

很简单，分析一下他们获取信息的途径以及内容，就有了答案。这些顾问拿到了惠普董事会成员和记者的姓名、地址、社会保险号、通话记录、电话账单记录以及其他一些信息。他们甚至使用一个记者的社会保险号建立了在线账户，以获取其私人通话记录。

惠普提交给其律师和内部法律人员的一份机密文件（详见www.social-engineer.org/resources/book/20061004hewlett6.pdf）的第32页列出了汤姆·珀金斯和惠普董事会成员的交流内容，其中包含一些有关伪装的内容。其中用到的部分策略列示如下。

- 他们将自己伪装成电信运营公司以非法地获取通话记录。
- 使用被调查者的身份来获取他们的私人通话记录。
- 利用非法获得的姓名、社会保险号和其他信息建立在线账户，从而获得他们的通话记录。

2006年9月11日，美国众议院能源和商务代表委员会给邓恩女士发了一封信（详见www.social-engineer.org/resources/book/20061004hewlett6.pdf），要求其提供所取得的所有信息。以下是他们列出的信息类型。

- 所有公布的和未公布的电话号码；
- 信用卡账单；
- 客户姓名和地址信息；
- 公共事业账单；
- 寻呼机号码；
- 手机号码；

- 社会保险号；
- 信用报告；
- 邮政信箱信息；
- 银行账户信息；
- 资产信息；
- 其他消费信息。

所有这些信息都是采用社会工程领域的灰色方法取得的。虽说是受雇做这种工作，但是他们所做的事情符合伦理道德吗？许多专业社会工程人员均不敢越雷池半步。从这一经典案例中，我们也能吸取一些教训：作为一名专业的社会工程人员，你可以模仿那些心存恶意的社会工程人员的方法和思维方式，却决不能堕落到他们那种地步。那群顾问犯的错误是：他们被授权去伪装、社会工程和审计惠普，但并没有被授权去审计美国电话电报公司（AT&T）、Verizon公司及公用事业公司等。在伪装的过程中，必须有明确的概要并且规划出哪些法律漏洞可以被利用，而哪些底线是决不能触碰的。

假如你是一名社会工程审计人员，可以就惠普这个案例展开关于政策、合同和原则等系列讨论，但这些内容不属于本章的讨论范围。使用本章所列出的原则有助于你作出决定，而且这些决定不会让你惹祸上身。

伪装成危险的、怀有恶意的身份盗用者，是社会工程渗透测试中合法的方式。测试、检查和验证你的客户的雇员不会落入恶意社会工程人员的陷阱，也可以帮你防御成功的伪装者。

### 4.3.3　遵纪守法

2005年，《私家侦探》杂志获得了对美国联邦贸易委员会金融实践部副主任乔尔·温斯顿（Joel Winston）的采访机会。他所在的部门专门负责规范和监测那些伪装行为（采访内容详见www.social-engineer.org/resources/book/ftc_article.htm）。

此次采访的要点列示如下。

- 据美国联邦贸易委员会定义，伪装是指使用诈欺、欺骗或者误导性问题来取得银行或消费者的信任，从而拿到财务情况等信息。
- 在美国联邦贸易委员会看来，使用已经获得的信息来确认目标身份的真实性是合法的，即便在该过程中采用了欺骗手段。但是社会工程人员不能利用这些从金融机构获取信息。
- 通过诈欺性的商业行为来获得电话清单或者手机通话记录被认为是非法的伪装行为。

美国联邦贸易委员会的官方网站澄清了本次采访的一些内容，并提供了如下补充资料。

- 任何使用虚假的、伪造的或欺诈性的陈述或文件，从金融机构窃取客户信息，或者直接从金融机构的客户那里骗取其信息的行为都是非法的。

- 任何使用伪造的、假冒的、丢失的或被盗取的文件，从金融机构窃取客户信息，或者直接从金融机构的客户那里骗取其信息的行为都是非法的。
- 任何指使他人使用虚假的、伪造的或诈欺性的陈述或文件，或者使用伪造的、假冒的、丢失的或被盗取的文件，从他人处骗得客户信息的行为都是非法的。

虽然联邦贸易委员会的焦点是金融机构，但其列出的指导方针也能提醒你在美国哪些伪装是违法的。了解当地的法律并且确保不会违法，对于专业社会工程人员来说非常必要。2006年，美国联邦贸易委员会对《FTC法案》第五条进行了补充，明令禁止使用伪装技术获取电话记录。

前面惠普案例中的五个私家侦探之一被指控为蓄意窃取身份罪，这项罪名相当严重。

保持伪装的合法性需要专业社会工程人员不懈的努力和研究，并且明确地计划要使用什么样的伪装。

排除之前提到的法律因素，利用可靠的伪装手段进入目标公司是最快的途径之一。然而，从本章的介绍也能够看出，伪装本身是要讲究天赋的，不只是戴上假发或者眼镜去冒充别人那么简单。

### 4.3.4 其他伪装工具

伪装时还有其他一些可利用的工具。

道具有助于让目标相信你的伪装。比如，车辆的磁性标志、配套的制服或装备、工具或者其他手提设备，还有最重要的——名片。

在我最近飞去拉斯维加斯出差的时候，名片的重要性震撼了我。我的笔记本包通常会被一遍又一遍地扫描，然后做除尘（炸弹尘埃或者别的危险物品）。我对这种安检从不反感，因为它们避免了我在空中被炸飞的可能，这点让我很高兴。

然而，我意识到90%的情况下，我都会引起安检人员的额外注意。这次出行比较特别，我忘记将开锁套装、RFID扫描器、4块额外的硬盘、万能钥匙（参见第7章）和一些用来进行无线入侵的工具从随身的笔记本包里拿出来。当这些东西从扫描仪器中通过时，我听到X光仪器的女操作员说："这些是什么？"

随后她叫来一个男同事看了看屏幕，他说："我也搞不清那些到底是什么。"他继而环顾四周，看到我在笑，便问道："是你的吗？"

我和他一起走到桌旁，他倒出我的RFID扫描器和专业开锁套装，问道："你怎么会有这些东西？干吗用的？"

显然我被问到了，但是在最后一秒钟我决定尝试一下。我拿出一张名片，说道："我是为网

络、建筑和人们做各种测试的安全专家，这些都是我的工具。”说着我递给他一张名片，他看了大概5秒钟说：“哦，不错。谢谢你的解释。”

他把我的东西整齐地放回去，把包拉好，就让我走了。通常，我还得通过炸弹探测器、小除尘机，然后被搜身，但是这次我得到的却是一句“谢谢”和快速放行。我开始分析原因，唯一的不同就是我递给他一张名片。当然，我的名片不是那种在线印刷的廉价商品，但令我没想到的是，这张名片在关键时刻充当了许可证，能够有效证实我的描述。

在接下来的4次飞行中，我特意把我所有的“黑客”装备放进我的包里，然后拿一张名片在兜里。每一次在安检时被问及这些东西时，我就递上名片。毫无例外，每次他们都向我道歉，把我的东西整齐地装回去，然后放行。

如果将我的经历想象成伪装。一些小细节可以让我说的话可信度大增，让我看起来正当并值得信任，而这一切只需要一张卡片，就可以让人相信我说的都是事实。千万不要低估名片的作用。友情提醒：印刷粗糙、看起来寒碜的名片的效果恰恰相反。一张背面印有“免费”广告的名片在专业伪装中不会起任何作用。不过，也没必要在这上面花费300美元，你完全可以用不到100美元让网上名片打印店打印少量精美的名片。

另一个需要认真对待本章的理由是，伪装通常是专业身份窃贼开始入手的第一步。鉴于身份盗用在最近犯罪中出现得比较频繁，知道它的原理并且能够有效鉴别，对于消费者、商务人员和安全专家来说都有很大的必要性。如果你是一位安全审计师，必须帮助客户提防这类威胁，并且针对可能的漏洞考验、测试他们。

## 4.4　小结

前文系统地介绍了伪装，并且提供了真实的案例。除此之外，本章还提及心理学原则也会影响伪装的方方面面。下一章将着重介绍和讲述专业社会工程人员如何使用心理战术成为精神控制专家。这点可以让每个社会工程人员向成功迈进一大步。

第 5 章

# 心理战术：社会工程心理学

我们看待事物的方式而不是事物本身，决定着一切。
——卡尔 · 古斯塔夫 · 荣格（Carl Gustav Jung）

在好莱坞电影和电视剧中，骗子和司法办案人员总是被描绘成具有神秘的才华。他们具有逃脱一切追查的能力，通过他人的眼睛就能识别出对方说的是谎言还是事实。通常我们会看到这样的场景：警察凝视着疑犯的双眼就可以判断出他是否在说谎，或者通过三言两语骗子就能令受害者拿出毕生积蓄。电影可能会让你相信操纵技术以及"让人们做任何事"都看似合理，甚至很简单。这些场景真的只是虚构出来的吗？可能获得影片中描绘的这种类似幻想的能力吗？

本章涉及的内容可以写成一本书，我将这些丰富的信息概括成了一些准则，而这些准则将改变你和他人打交道的方式。本章涉及的一些话题是以一些极为聪明的研究者在各自领域的研究成果为基础的，这些话题中讨论的技巧也都在社会工程的环境下经过了缜密的测试。例如，微表情这一话题就是以世界著名的心理学家和研究学者保罗 · 艾克曼博士的研究成果为基础的，他利用自己的天赋开发出的解读人们面部表情的技术，改变了司法人员、政府官员、医生以及普通人与他人交往的方式。

神经语言程序学的鼻祖理查德 · 布兰德勒（Richard Brandler）和约翰 · 葛瑞德（John Grinder）提出的一些理论，改变了人们对思维模式和语言重要性的认识。这些都是相当具有争议的领域，本章将揭开其神秘面纱，并且讲解其在社会工程中的应用。

一些最优秀的审讯者开展了培训工作，并开发了相关的框架，帮助执法人员学习怎样有效地审讯嫌疑人。这些原则和方法具有深厚的心理学基础，学习这些方法可以正确解读目标的思维方式，攻破他们的心理防线。

正确地解读人们说话、手势、眼神和面部表情中的信号，可以使你看起来像一位精通读心术的人。本章将细致阐述这些技巧，以供专业社会工程人员使用。

亲和力是销售培训人员和销售人员经常提到的字眼，这是获取信任、显示信心的一个非常重要的方面。本章将介绍如何在短时间内与目标人物建立友善的关系，真正提高社会工程人员的技能和水平。

本章以我个人对人类思维攻击的研究成果收尾。缓冲区溢出通常是由黑客编写的程序，通过宿主程序的正常使用，可以利用它执行通常带有恶意目的的代码。一旦运行起来，程序会按照黑客预先设定好的步骤执行任务。那么如果可以在人类的大脑中执行“命令”，让目标按照我们的要求行动、给出我们想要的信息，会怎么样呢？这样是不是就可以证明人的思维是可以被操纵的呢？

这一强大的信息当然也会被用来达到恶意目的。我以这种方式将此信息公布于众，目的在于揭开“坏人”的面纱，剖析他们的手段、思路和准则，然后一一进行分析，让读者学会如何识别他们的真面目。将这些技术公开出来，有助于大家轻松识别、抵御及缓解这种攻击。

学习本章所涉及的数据和准则需要读者不停地转换思维。模仿、学习并研究这些方法不仅能够提高你的安全能力，还能够改变你和他人沟通及交流的方式。

当然，本章并不能涵盖这些技巧的所有方面。我提供了一些有助于你强化这些技能的链接或者建议。本章不仅是行为指南，更为社会工程奠定基础，为你指明方向，从而在日后不断强化社会工程技巧。

社会工程技巧的学习并非一蹴而就之事，所以要有耐心。这些技巧的学习需要花费几年的时间，如果要达到专业级别，更需要很多实践的磨练。当然，你可能很快掌握一些特定方面的技巧，如果不能很快掌握的话，也不要放弃。只要功夫深，铁杵磨成针。

在进入本章的正式内容之前，下面将会做一些准备工作，说明为什么这些原则会起作用，以及它们是如何起作用的。我们必须要理解人类的思维模式。在对人们吸收和处理信息的模式理解得更为透彻后，你就能开始理解这一过程背后的人类情感、心理学和身体表示。

## 5.1　思维模式

要改变某人的思维方式，必须要理解人们的思维方式和思维模式。逻辑上，这是进行这方面社会工程尝试的第一步。

听上去好像我们得成为心理学家或者神经学家才能理解人们思维的方方面面。纵然那会有一定的帮助，但其实没那个必要。通过一些研究和实际应用，就能深入人类思维的内部工作机制。

2001年8月，美国联邦调查局（FBI）发布了一份司法公告（详见www.social-engineer.org/wiki/archives/ModesOfThinking/MOT_FBI_3of5.htm），其中包含一些人类思维模式的深入阐述，具体如下。

> 让客户认可你的非言语行为、用客户认可的语言表达方式，并且在音量、语调和方言上相匹配，这样通常可以免吃闭门羹。

上面这句话虽简单，但是其中包含的内容却很多。一般来讲，如果能够迅速摸清目标的主导思维模式，然后通过微妙的方式进行确认，就可以令其在告知你哪怕是私密信息时，降低戒备，打开心扉。从逻辑上来讲，这时也许你会问："怎样才能识别目标的主导思维模式呢？"

即使问目标自己这个问题，也不一定能够得出一个清晰的答案，因为很多人并不清楚自己到底是何种思维模式。因此，社会工程人员必须掌握特定的工具才能识别他人的思维模式，然后快速切换到对应的模式。方法和途径有现成的，但是首先必须要了解其基础。

### 5.1.1 感官

对于认知的价值问题，哲学家已经争论了几个世纪了。有些人甚至认为，现实并不是"真实"的，它只是我们的感官带给我们的认知。就个人而言，我并不赞同这种思想，但是我相信这个世界是通过感官进入我们的大脑的。人们通过解释这些感官获得对现实的认知。传统的分类方法中，感官通常分为5种：视觉、听觉、触觉、嗅觉和味觉。

人们倾向于钟爱这些感官中的一种，也就是说某种感官会占据主导地位，这也是人们记住事物的方式。通过一个练习就能确定自己的主导感官，闭上眼想象你清晨起床的画面，你能记得的第一件事是什么？

是温暖的阳光照在脸上的感觉吗？是配偶或小孩叫你的声音吗？你清楚地记得楼下咖啡的香味吗？抑或是嘴里并不清新的口气，提醒你需要刷牙了？

当然，这一实验并不能完全确定，可能要尝试好几次才能真正意识到自己的主导感官。我曾经和一对夫妇说起过这一概念，他俩的反应很有意思。妻子醒来的第一反应是看看时钟，担心自己快迟到了，而丈夫则是每次都翻个身，发现妻子不在身旁。几个问题之后，基本上可以确定丈夫是动觉类型的，或者说其主导感官是触觉，而妻子则是视觉占主导地位。

以上只是测试，实际工作中你不可能直接走向目标说："闭上眼，告诉我今天早晨起床后你做的第一件事是什么。"除非你伪装成家庭医生，否则肯定会吃闭门羹。

那么，如何才能在避免尴尬询问早晨起床习惯的情况下得知目标的主导感官呢？

### 5.1.2 3种主要的思维模式

尽管我们有5种感官，与思维模式相联系的只有其中的3种：

- 看到，也就是视觉思维者
- 听到，也就是听觉思维者
- 触到，也就是动觉思维者

每种感官都有各自起作用的范围，或者说有各自的*次感元*。声音太大或者太轻？光线太亮或者太暗？环境太冷或者太热？拿实际例子来说：直视阳光会感觉太过刺眼，喷气式发动机的声音太过震耳，零下30度（华氏）感觉太冷等。伊万・巴甫洛夫做过一个实验，每当给狗喂食时，他就摇手铃。最后狗一听到铃声就会流口水。然而，大多数人不知道的是，伊万更为感兴趣的是次感元引起的生理和情绪反应。有趣的是，铃摇得越大声，狗的口水流得越多。次感元的范围变化引起了身体的直接变化。欲详细了解巴甫洛夫的研究和他的全部演讲，请参见www.ivanpavlov.com。

尽管人和狗有很大的不同，巴甫洛夫的这项研究对于理解人们的思维模式还是很有价值的。我们中的很多人可能同时具备3种思维模式，但是占据主导地位的只有一种——“响声”最大的那个。甚至在主导思维模式下，主导感官的深度也会有所变化。

下面我们将深入地探讨每种思维模式的一些细节。

#### 1. 视觉

大多数人通常都是*视觉思维者*，这种人通常记得的是事物的面貌。他们能够清晰地记住场景——颜色、纹理及光线的明暗等。他们能够清晰地描述过去的事件，甚至能构建未来事件的图像。当面对一些事物的时候，他们需要看到一些东西才能作决定，因为视觉输入直接与他们的决策相关联。很多时候，视觉思维者会依据在视觉上吸引他们的东西，而不是对他们来说真正“更好”的东西来作出决定。

尽管男人更可能是视觉思维者，但并不是说所有男人总是视觉导向的。虽然视觉营销或者视觉效果通常会对男人有吸引力，但不要以为所有男人都是视觉思维者。

视觉思维者在谈话中经常使用特定的词汇，例如：

- “我明白你的意思。”
- “我看那挺好。”
- “我大概有点印象了。”

对于视觉思维者来说，主导感官的工作范围具有一定的特征，通常这些也称为次感元。例如：

- 光线（明/暗）
- 尺寸（大/小）
- 颜色（黑白/彩色）
- 运动（快/慢）
- 焦点（清晰/模糊）

尝试在没有视觉输入的情况下与视觉思维者进行争论、协商，向其推销，操纵或者影响他，基本上会毫无效果，至少会非常困难，因为视觉思维者需要视觉输入才能作出决定。

### 2. 听觉

听觉思维者会记住事件的声音。他们会记住闹铃声音太大、女人的窃窃私语、孩子甜美的童声或者家犬惊悚的吠声等。对声音敏感的人通过倾听能够学得更好，而且相比于用眼睛看，别人告知他们事情时，他们能够获取更多的信息。

因为听觉思维者总是能记住事物发声的方式，或者说声音能够唤起他们的记忆，所以他们经常使用这样的表述：

- “宏亮并且清楚……”
- “这件事情告诉我……”
- “听起来不错。”

听觉主导感官的次感元范围如下：

- 音量（大/小）
- 音调（高/低声部）
- 音准（高/低）
- 节拍（快/慢）
- 距离（远/近）

在面对听觉思维者时，一定要注意自己的措辞。他们听到的词语表达将决定事情的成败。我见过因为用词不当而让会面效果从巅峰跌入低谷的遭遇，因为对方是听觉思维者。

### 3. 动觉

动觉思维者特别在意感受。他们能够记住事件给自己带来的感受：温暖的房间、拂过肌肤的清风、令他们惊恐而跳起的电影。动觉思维者通常会用自己的双手去感知物体。仅仅告诉他们某物柔软不如让他们触摸一下。但帮他们回忆曾经摸过的柔软的物体，可以让他们想起非常真实的情感和触感。

“动觉”这一词汇与触觉、本能以及身体的本体感觉有关，简单点说，就是身体在空间中所处的位置，以及事物让他感受到的自我意识。动觉思维者使用如下表述方式：

- “我能抓住那个想法的要点。”
- “那个是如何抓住你的？”
- “我会联系你的。”
- “我刚想联系来着。”

- “这感觉怎么样？”

动觉思维者的次感元范围如下：

- 强度（强/弱）
- 面积（大/小）
- 质地（粗糙/光滑）
- 温度（热/冷）
- 重量（重/轻）

帮助动觉思维者回想起与某一事物相关联的感觉或者情感，可以让那些情感再现。对于非动觉思维者来说，动觉思维者可能是最难应对的，因为他们对景象和声音都不会有反应。社会工程人员要想与他们沟通，得和他们进行感觉上的联系。

理解以上这些基本原则，能够帮助你快速辨别出对方是何种类型的思维者。再次回到原来的问题，在不询问对方早上起来的第一感觉的情况下，如何判断他的主导感官呢？就算判断出来又怎样呢？有那么重要吗？

#### 4. 辨别目标的主导感官

想要确定对方的主导感官，首先尝试自我介绍，然后开始简短的交流，在此过程中留意对方所说的话。在你走向目标对象并和他打招呼时，也许他都没有正式地看着你。可能他比较无礼，也可能他不是一个视觉思维者。视觉思维者需要看着对方说话才能正确沟通，这种行为似乎证明他不是视觉思维者。这时，你可以再简单地问一句：“今天的天气让人感觉很舒服啊！是不？”观察他的反应，特别注意他是否会面露喜色。

也许你可以戴一个大的、闪亮的银戒指，谈话时不断地打手势，也许你会看到戒指引起了他的注意。他会不会感兴趣地伸手触摸，甚至想要拿在手里仔细看看？动觉思维者遇到这种东西会很想触摸。我认识一位女士，她是一个很明显的动觉思维者，每当看到自己认为质地柔软或高品质的东西时，她必须要摸一摸。她会说：“哇哦，那件毛衣看起来好柔软啊！”从这句话来看，我们可能认为她是视觉主导的，然而后面发生的事却证明了她是动觉思维者——她径直走过去，用手去摸毛衣、去感受。这个女人在去商店购物时必定会摸一下每件商品，不管她是否需要。通过触摸物体，她和商品之间建立了联系，这种联系让她觉得很真实。通常她对那些没有亲手碰触过的物品很难产生深刻的记忆。

用一些关键主导词来提问，观察目标的反应，然后认真地听他的回答，这样就能判断出他的主导感官。如果听到诸如看、瞧、亮及暗等字眼，可以表明目标是一位视觉思维者。当然，就像前文所述，这并不完全准确。并不存在一个通用规则。每一条线索都能够为你指明方向，从而据此提出更多的问题进行验证。友情提醒：如果使用与对方思维方式不同的模式进行交流，可能会让对方觉得不悦。不停地提问来确定一个人的思维模式，会令对方反感，因此在交流过程中，应

当注意尽量少问问题，多进行观察。

#### 5. 为何了解思维模式如此重要

我曾和一位名叫托尼的人共事，他能够把水卖给将要淹死的人。托尼非常相信可以在销售工作中找出并利用对方的主导感官。他使用的一些方法值得我们借鉴。在第一次与目标人物会面时，他总是拿着那支很炫的、闪闪发光的钢笔，并打很多手势，观察目标的视线是否会跟随那支笔移动。如果有一点的话，托尼就会加大动作幅度，看他的目光是否会进一步跟随。如果在前几秒中未见成效，他会将笔帽不断开合，发出咔嗒声。声音不是很大，但足以干扰一个人的思绪。如果他是视觉思维者，就会引起他的注意。这招一旦奏效，托尼就会在对方每次认真思考时都这样“开合”一次，使得目标对这种声音和当时说的话产生心理上的反应。这招再行不通的时候，他会将手伸过桌面，轻拍对方的手腕或者手臂，或者如果坐得足够近的话，就会拍拍他的肩膀。当然他不会安排过多的这种肢体接触，他的目的是看目标人物的反应：是会害羞地躲开，比较乐意地接受，还是觉得自己被打扰了。

通过这些微妙的方法，他能够快速地判断出对象的主导感官最可能是哪一种。整个过程不会超过60秒。在发现期待的信息之后，他便会将后续的对话转移到主导感官领域，甚至通过谈话中的言辞、举止和响应体现出来。我见过的人当中，没有比托尼更会推销的了。认识他的人常说：“我感觉托尼很清楚地知道我的需求。”

托尼始终能够以目标人物自己喜欢的方式来愉快地聊天。如果目标是视觉思维者，托尼会用下述表述方式：“你看这个怎样？”他会使用一些诸如“看得见”的东西或者可视化的场景，令他们感觉处在一种非常舒适的氛围中。

人们在舒适的氛围中会备感放松。在社会工程过程中越是能将人们置于舒适的氛围，成功的几率就越高。人总是喜欢和让他感到舒适的同伴在一起，这是人的本性使然。举个例子，如果某人让你备感“温暖和贴心”，或者能够听懂你的话，或者能听出你的口音，你会轻易地信任他、向他敞开心扉，并允许他进入你的生活圈。

我想重申这个观点：识别并利用他人的主导感官并不是一门精密的科学。社会工程人员只能把它当做众多工具中的一种，不能完全依赖它，把它神化或者当成科学。某些人类本性方面的心理学知识是有一定科学依据的，具有一定的可靠性。事实上，其中有些会给人以深刻的印象，让你能够读懂别人的心思。有的在业界还存在一定的争议，有的则广为心理学家、执法部门和社会工程人员所认同。下一节会从微表情入手，就此进行深入探讨。

## 5.2 微表情

对于面部表情的解读，大家可能已经很熟悉了。人们的喜、怒、哀、乐等各种情绪都会通过

面部表情体现出来。如果有人使用虚假的表情呢，比如假笑？在集市上遇到不太喜欢的人时，我们会面带“微笑”地说：“约翰，真高兴在这里碰到你。替我向莎莉问好。”

我们可能表现得非常开心和兴奋，内心却很愤怒。面部那种长时间持续的表情叫做*宏表情*，一般情况下，这种面部表情更易于传达情绪。与微表情类似，宏表情也是由情绪控制的，但是并非自然流露，经常能够伪装。

几个研究人类行为的先驱花费了几十年的心血来研究并尝试理解人类是如何传达情感的，并最终将之命名为*微表情*。

微表情是情绪的自然反应，不大容易控制。情绪触发面部特定肌肉的反应，形成特定的面部表情。很多时候，这些表情的持续时间不过1/25秒。因为这些表情都是情感反应引发的无意识的肌肉运动，所以几乎不可能被人为控制。

这一定义也并不是首次提出的，1872年，查尔斯·达尔文在他的著作《人类和动物的情绪表达》（*The Expression of the Emotions in Man and Animals*）中提到过面部表情的通性和每种面部表情对应的肌肉运动。

20世纪60年代初期，两位研究员哈格德（Haggard）和艾萨克斯（Isaacs）最先发现了现在所称的“微表情”。1996年，他们在著作《面部微表情瞬间——心理的自我反应机制》（*Micromomentary Facial Expressions as Indicators of Ego Mechanisms in Psychotherapy*）中，阐明了发现“微瞬表情”的过程。

同样在20世纪60年代，人类行为学先驱威廉·康登（William Condon）花费了大量的时间，对长达几小时的磁带进行逐帧研究，发现了人类表情的“微运动”。他还在神经语言程序学（后期对此研究比较多）和肢体语言领域做过深入的研究。

或许微表情领域最具影响力的研究者之一就是保罗·艾克曼博士。作为先驱，艾克曼博士将微表情发展成今天的一门科学。他研究微表情40多年，获得了研究科学家奖，并于2009年登上《时代》杂志，成为年度最具影响力人物之一。

艾克曼博士和心理学家希尔文·汤姆金斯（Silvan Tomkins）一起研究面部表情，发现了与主流观点不同的研究成果：情感不是由文化决定的，而是在不同文化和物种间普遍存在的。

他和莫林·奥沙利文博士（Dr. Maureen O’Sullivan）策划出一个叫“巫师”的项目。他是将微表情运用于测谎方面的先驱，他们对15 000个来自各行各业的不同文化背景的人进行测试，发现在不经过专业训练的情况下能够躲过测谎仪的只有50人。

20世纪70年代，艾克曼博士开发出一套面部表情编码系统（Facial Action Coding System，缩写为FACS），用来对人类可能的表情进行标记和编码。这套系统不仅涵盖各种面部表情，还包括欺骗时整个身体的反应。

1972年，艾克曼博士将与最基本的、生物共有的情绪相关的表情列示了出来，包括：

- 愤怒
- 厌恶
- 恐惧
- 快乐
- 悲伤
- 惊讶

艾克曼博士的这些研究成果得到了推广，很多执法部门和企业开始应用他在测谎方面的成果。1990年，他在一篇名为“基本情绪”（Basic Emotions）的论文中对他之前的清单进行了修订，将情绪划分为积极的和消极的两种（详见www.paulekman.com/wp-content/uploads/2009/02/Basic-Emotions.pdf）。艾克曼博士还撰写了很多关于情绪、面部表情和测谎的书籍，帮助人们理解面部表情解码的价值。

从前面简短的介绍中不难看出，微表情并不是空穴来风。相反，它是人类行为学领域一代代博士、研究员、专家花费无数时间研究出来的成果。作为一名社会工程人员，懂得观察微表情可以有效地保护你的客户，教他们发现骗局中的微小漏洞。

如果你是一名社会工程人员，或者是对微表情感兴趣的人，我强烈建议你读一读艾克曼博士的书，特别是《情绪的解析》（*Emotions Revealed*）和《解密脸部：从脸部线索识别情绪的指导》（*Unmasking the Face*）。他是该领域真正的权威。接下来将对微表情进行简单的阐述，告诉你作为社会工程人员，如何将其运用到工作中。

前文提到艾克曼博士列出了6类主要的微表情，后来他又将“轻蔑”添加进来，变成了7类。下面将逐个进行介绍。

### 5.2.1 愤怒

愤怒和其他表情相比，通常是比较容易识别的。人在生气的时候会紧抿双唇、眉头紧锁，当然还有最为明显的特征：双眼圆瞪。

愤怒是一种比较强烈的情绪，它能够触发很多附带情绪。有时候当一个人对某件事情感到生气的时候，你会看到如图5-1所示的微表情。比较难以察觉的原因是这种面部运动可能只会持续1/25秒。

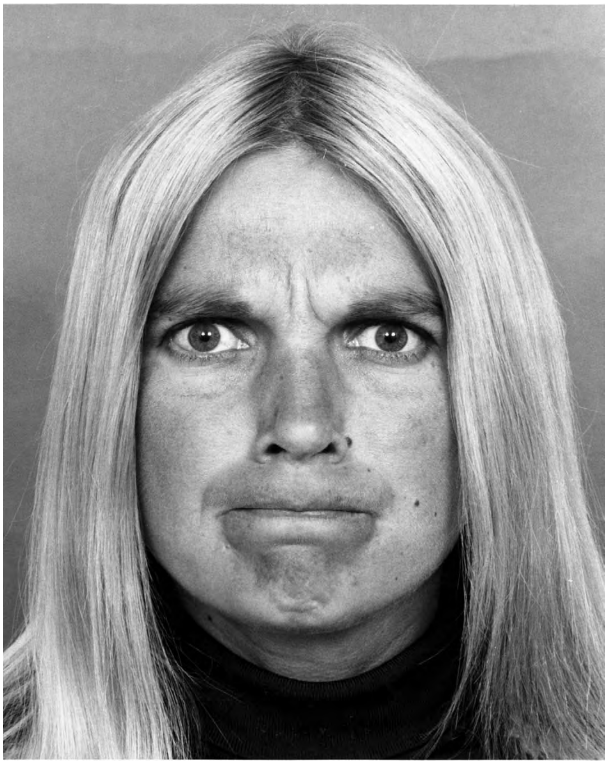
学会查看特定的微表情可以大大提升理解他人的能力。关于如何掌握这种能力，艾克曼博士建议大家自己做相应表情的练习，可以参考以下的步骤。

(1) 把眉毛往下拉，使其并拢到一块。仿佛是要使眉毛能够触碰到鼻子。

(2) 当眉毛下压的时候，尝试在眉毛不动的情况下，使劲睁大眼睛。

(3) 紧闭双唇。不要撅起来，只是让上下唇紧紧地抿在一起。

(4) 瞪眼。



该图片由保罗·艾克曼博士提供

图5-1　注意瞪圆的双眼、紧抿的嘴唇和紧锁的眉毛

你感受到什么样的情绪？我第一次尝试的时候，感到异常愤怒。接下来提到的是本章的要点。

> 如果制造出面部表情可以引发一种情绪，那肯定意味着面部移动可以影响我们感受到的情绪，甚至可能感染周边的人。

对着镜子持续练习这种表情，直到做对为止。图5-2所示的就是西蒙·考威尔（Simon Cowell）展示出来的一种非常典型的愤怒表情。

该图看起来可能没有图5-1那么明显，但是从他的脸上可以识别出与愤怒相关的所有微表情。

拥有熟练掌控微表情的能力对有效理解这些表情背后的情绪十分有用。当能够成功做出并解码微表情，你便能够理解引发这种表情的情绪。这样你就能够明白对象的精神状态。不仅要能够

做出各种微表情，还要主动解读周边人物的表情，这会对你控制社会工程活动的成果大有裨益。



图5-2 西蒙绝对是愤怒了，注意他的表情

### 5.2.2 厌恶

厌恶通常是对你确实不喜欢的东西产生的一种强烈的反应。这种“东西”不仅限于物理实体，有的时候也可能是一种信念或者感觉。

极为讨厌的食物会令你产生厌恶的感觉，就会触发这种微表情。不可思议的是，即便在没有闻到或看到这种食物的时候，想到它都会引发同样的厌恶情绪。

十几岁的时候，我和几个朋友一起去迪士尼乐园。我当时并不喜欢也不想去玩过山车，然而最终还是招架不住朋友的劝说，去了太空山——一个室内过山车项目。快到一半时，还觉得过山车对我来说其实也没什么，但突然发现身上沾了一些湿湿的恶心的东西，然后就是一股恶心的气味令我作呕。不仅是我，身后的很多人也有类似的反应，可以说基本上没有人能忍住不吐。很快地，大家几乎同时呕吐在了另一辆“未来世界”列车的车窗玻璃上，该项目是为了让游客在行驶缓慢的列车上体验太空山之旅。让我们吃惊的是，乘坐“未来世界”列车缓慢在园中游览的旅客看到车窗上的呕吐物时，竟然也开始呕吐了，尽管他们并未闻到或接触到窗体外

我们的呕吐物。这是为何？

厌恶。体液通常会让人产生厌恶的感觉，这也是你读上文时可能已经开始觉得厌恶的原因之一。

厌恶通常表现为上唇上启、露出牙齿，鼻子皱成一团。有时随着鼻子皱起，双颊会上移，感觉想阻隔难闻的气体进入鼻腔或者阻断恶心的想法进入自己的私人空间。

有一次我在看一篇关于冬奥会的文章，一张叶卡捷琳娜·尤金娜（如图5-3所示）的照片就清晰地显现出厌恶的特征。注意观察她那上抬的嘴唇和皱起的鼻子。她是在看自己的得分吗？被对手打败了？我不确定，但她正在看的东西一定令她感到不快。



图5-3　皱起的鼻子和上启的嘴唇是厌恶的明显表征

根据艾克曼博士的研究，厌恶是一种情绪，它是肌体对于看起来、闻起来甚至想起来觉得恶心的事物的一种反应。从社会工程的角度来看，这种情绪可能会导致失败，然而这些反应可以帮助你判断自己是否已达到目的或者是否已经引起目标的反感和排斥。

一般情况下，不论是什么原因导致你的目标产生了这种表情，都宣告了你的失败。如果你的外表、体味、风格、气息或者其他方面让他人感到厌恶，那么大多数情况下你已经失败了。你必须意识到目标的好恶。例如，如果审计的对象是一个知名的律师事务所，而你身上有很多穿刺或纹身，就会给目标带来强烈的反感，这可能直接将你的社会工程行动扼杀于摇篮。当你看到如图5-4所示的表情时，就要做好离开的准备了。

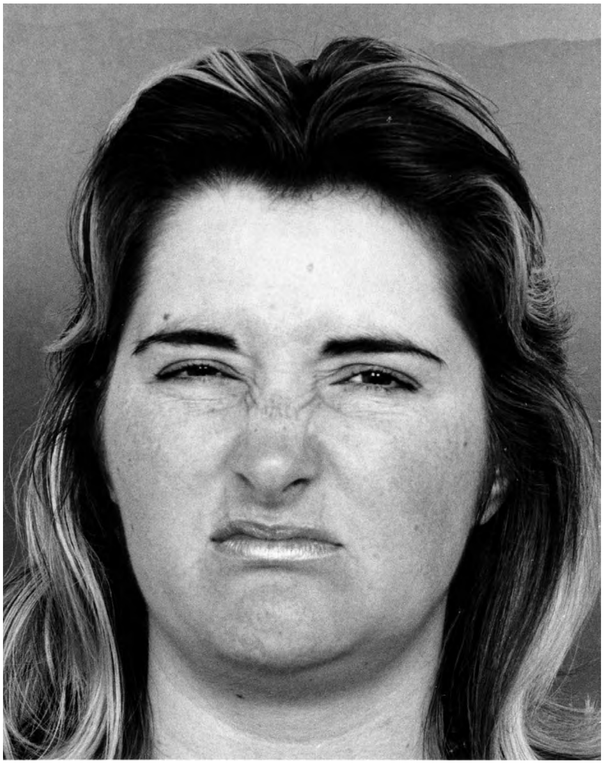


图5-4 如果看到这种表情，就说明有问题了

在伪装时，必须认真考虑你的外表。一旦发现目标脸上出现厌恶这种强烈的负面情绪，较好的方式是赶紧放弃，礼貌地为自己开脱后，考虑一种新的伪装或者另辟蹊径。

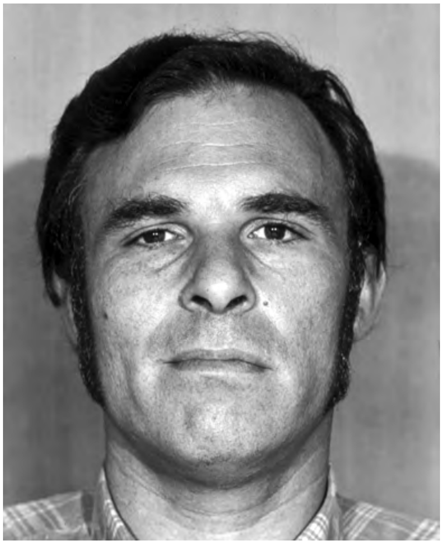
### 5.2.3 轻蔑

轻蔑是一种很强烈的情绪，通常会与厌恶混淆，因为两者具有紧密的关联。艾克曼博士甚至在起初的基本情绪列表中没有写上轻蔑。

在艾克曼博士的《情绪的解析》一书中，他做过如下描述："轻蔑只是针对人或者人的行为，而不是针对味觉、嗅觉或者触觉。"他举了个吃牛脑的例子，你可能会因为这种想法而觉得恶心，这就会引起厌恶。而看到正在吃牛脑的人时，就会触发"蔑视"，不是对这种行为，而是针对吃牛脑的那个人。

在我看来，这一点非常重要，理解该微表情也很重要。蔑视通常针对的是人，而不是具体的物体，这对我们理解这种微表情所表达的含义非常重要。如果能够看出目标对象是否带有轻蔑的表情，就能帮助我们更清晰地找出他产生这种情绪的真正原因。

轻蔑的表情一般伴随着皱起的鼻子和上启的上唇，但只会出现在脸的一侧，而在厌恶的表情中，整个鼻子都会皱起，整个上嘴唇都会上启。从图5-5中就能看出一丝细微的轻蔑表情。



该图片由保罗 • 艾克曼提供

图5-5　请注意观察艾克曼博士的脸——微皱的鼻子和上移的右脸

尝试模仿“轻蔑”的表情。如果你像我一样，过不了多久就会感到心中产生的愤怒和轻蔑的情绪。做这种模仿练习，并且观察这种模仿给情绪带来的影响是件有趣的事情。

在图5-6中，小威廉姆斯（Serena Williams）明显表现出了轻蔑的特征。我从网上找到的这张图片，但是没有将整篇新闻稿保存下来，因此并不知道她轻蔑的对象是什么。但是不管是什么，她明显对其感到不爽。




图5-6　小威廉姆斯的左脸表现出了轻蔑

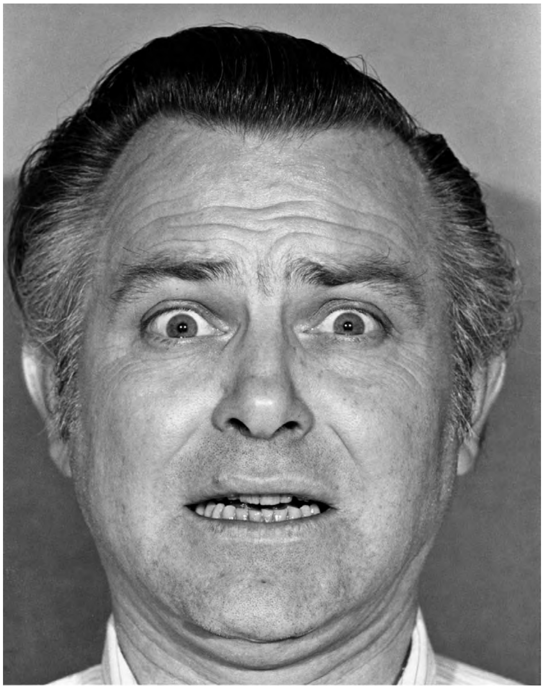
让人们产生轻蔑情绪的事情也会触发强烈的负面情绪，因此轻蔑通常会伴随着愤怒。轻蔑是和他人打交道时要尽量避免的情绪，尤其是在社会工程过程中。

### 5.2.4 恐惧

人们经常混淆恐惧和惊讶，因为这两种情绪引起的面部肌肉运动非常相似。最近在飞机上，我正准备写“快乐”那节，但当时发生了些意想不到的事情，直接导致我撰写了“恐惧”这节。

我身高6英尺3英寸（约1.9米），不矮也不瘦。坐在飞机上，想到还有几个小时要打发时，我决定利用这段时间来工作。这里我要插一句，当时的经济舱座位有些不同。我坐下后，打开笔记本电脑，看着外面的天空，开始思考如何撰写“快乐”一节的开头。不一会儿，我就决定写“恐惧”，因为旁边的乘客拿出一瓶水喝了一大口，但没盖上瓶盖。我用眼角的余光看到瓶子从他手中滑落，倒向我的键盘。我当时的第一反应就是“恐惧”。

我瞪大双眼，皱起眉毛，嘴唇同时向耳朵拉起。当然，事发当时，我并没有意识到这一切的面部变化，但是后来在对发生的事情进行回想和分析时，我知道自己当时感到的是恐惧。我分析了自己当时面部肌肉的移动方式，得以确定如果我不断重复这样的表情，会体会到相同的情绪。我确定自己当时的表情和图5-7所示的表情类似。



该图由保罗·艾克曼博士提供

图5-7　恐惧的明显特征

请尝试以下步骤，看你能否产生同样的情绪。

(1) 使劲往上抬眉毛。
(2) 缓缓张开嘴巴，向后咧开嘴角。
(3) 如果可以的话，在眉毛上扬的过程中努力使它们皱在一起。

感觉如何？你的双手、手臂还有胃有什么感觉？是不是感到有点害怕？如果还没有，再试一遍，只是这次尝试去想象一个你控制不了的情景（类似我在飞机上的那段经历，或者是伴随着轮胎尖锐的摩擦声，前方车辆紧急刹车）。这时感觉怎么样呢？

通常情况下，你会感到害怕。我从网上找到一张带有明显恐惧特征的照片（参见图5-8），照片里的人是美国参议员奥林匹亚·斯诺（Olympia Snowe）。暂不管拍下该表情之前她被问了什么问题，她的恐惧表情从照片中一眼就能辨别出来。她的眉头高高抬起，双唇向后微张，而且上扬的眉毛几乎皱到了一起。



图5-8　斯诺参议员明显的恐惧表情

从一名社会工程人员的角度来看，恐惧经常被用来诱使目标对象做特定的反应和动作。具有恶意动机的社会工程人员通常会对毫无戒备心的用户运用这种伎俩，从而诱使他们点击特定的图标或者泄露有价值的信息。例如，有些恶意的提示词如下："你的电脑感染了病毒，点击这里进行修复!!"这些标语对于不懂技术的人百试不爽，他们会由于担心中毒而点击进去，结果电脑就真的感染了病毒。

我曾经合作过的一家公司就被一名心怀恶意的社会工程人员攻入了，他当时利用的就是员工的恐惧心理。在得知公司的CFO出城参加一个重要的商务会议，期间不便被打扰后，该社会工程人员伪装成一名技术支持人员混进了公司。他要求进入CFO的办公室，但被拒绝了。然后他使用了如下伎俩："你们的CFO史密斯先生打电话给我，叫我在他出席会议的这段时间帮他把电子邮箱的问题处理好，如果在他回来之前解决不了，后果会很严重。"

秘书担心如果不把CFO的电子邮箱问题解决，自己会受责罚。她的老板会不会大发雷霆？她

会不会因此丢掉工作？鉴于对不良后果的担忧和畏惧，秘书让这位“技术支持人员”进去了。如果该社会工程人员经验丰富，他可能就是通过观察秘书的面部表情得知了她的心理动态，通过不断强化她的担忧和紧张，使她达到恐惧的状态，从而实现自己的目的。

恐惧是一种强大的推进器，可以使你或者目标对象做出异于平常的事情。

### 5.2.5 惊讶

如前文所述，艾克曼博士和微表情领域的其他心理学家认为惊讶和恐惧有着密切的联系，因为从表情上来看二者存在很多相似的地方。尽管如此，二者还是有些明显的不同，例如嘴唇移动的方向和眼睛反应的方式。

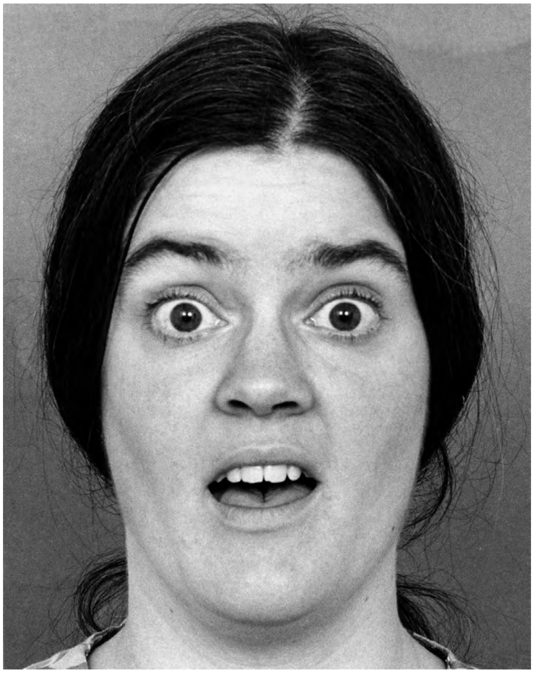
请试着做以下动作来练习“惊讶”。

(1) 抬起眉毛，不是充满恐惧而是抱着想尽量睁大眼睛的目的去做。

(2) 轻轻地张开下颚。

(3) 练熟这个表情以后，试着加快速度。

我注意到自己做这种动作的时候不经意间吸了不少空气，这让我感到一种类似于惊讶的情绪。你应该会看到类似于图5-9所示的表情。



该图由保罗·艾克曼博士提供

图5-9 注意眼睛和双唇是不是与恐惧的表情类似

令人感到惊讶的可能是好事情，也有可能是不好的消息。听到女儿牙牙学语时蹦出的字眼当然是件令人吃惊的好事情。某些意料之外的事情、通知或者问题也可能导致惊讶的反应。

这便是我对于图5-10中杰西卡·辛普森（Jessica Simpson）的表情所传达的内容的猜想。注意观察她上扬的眉毛和张开的下颚。她表现出来的惊讶特征较为明显，可能刚被问到了一个令她感到吃惊的问题，或者是听到了什么震惊的消息。



图5-10　除了一些细微的差别，惊讶经常会被误认为是恐惧

如果是积极的惊讶，通常会引发一丝微笑或快乐的表情。如图5-10所示，从杰西卡的表情不难看出，她不仅是惊讶，而且还带有一丝惊喜在其中。社会工程人员有时会利用惊讶来打开目标对象的心门，比方说，机智的对答或不经意间的玩笑可能会使目标马上放松警惕，降低其心理防线。

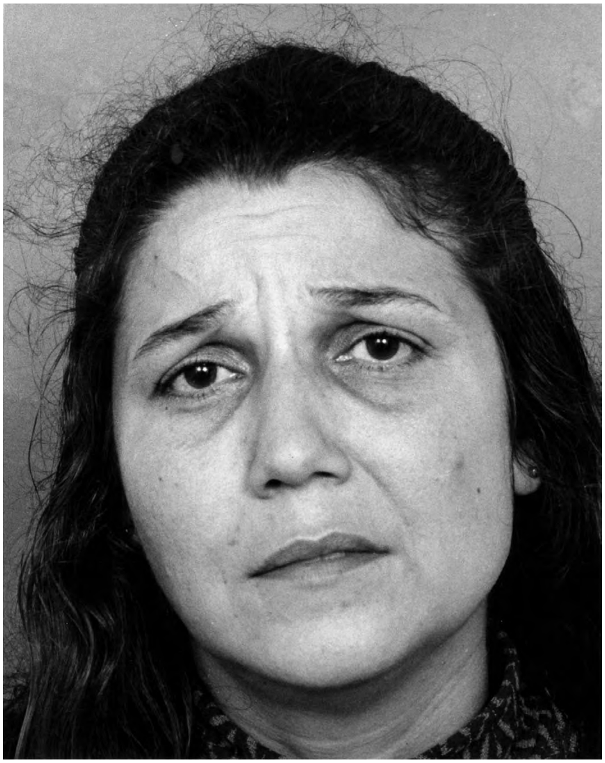
## 5.2.6　悲伤

悲伤是一种强烈而极端的情感。我们看到他人悲伤，很容易心生怜悯，感同身受。有些人看到别人悲伤，自己就会产生悲伤的情绪，甚至也会哭泣。

通过以下练习，很容易产生悲伤的感觉。

(1) 轻轻地张开嘴巴。
(2) 下咧嘴角。
(3) 保持嘴唇不动，同时上抬你的双颊，感觉自己眯着眼睛。
(4) 保持表情不动，眼睛往下看，让上眼睑无力地下垂。

通常这个时候，你便会产生悲伤的情绪了。我第一次做这个表情的时候，就立刻奏效了。我发现自己得控制练习这个表情的时长，因为练习带来的悲伤会持续较长的一段时间。图5-11展示的便是“悲伤”的表情。



DR. PAUL EKMAN对应：该图片由保罗·艾克曼博士提供

图5-11 注意双唇和下垂的眼睑，这意味着悲伤

悲伤的另一个特征使它成为一个奇妙的情感，即它并不需要显现出极度的痛苦或悲伤。悲伤可以表现得非常微妙，可以用局部的面部表情来传达。人们可能会试图使用虚假的微笑或者“坚忍的眼神”隐藏悲伤——凝视正前方，面容呆滞，但你可以看出他们正试图控制内心的真实感觉。

请看图5-12，图中展现的就是这种表达方式的悲伤。在对凯特·戈瑟兰（Kate Gosselin）的

一次有关离婚和家庭的采访中，她极力地隐藏自己内心的情绪，然而如果仔细观察她的双唇，你就会发现一些细节之处体现了她内心的悲伤。



图5-12　注意双唇咧向后下方，这意味着悲伤

除了双唇，眼睛是传递悲伤的另一个关键信号源。这种表情有时难以发现，甚至会被误认为是疲劳或者其他情绪，不过通过观察他的行为举止和肢体语言可以找到一些线索。

遮住大部分脸的这种文化充分体现了这一点。如图5-13所示，一群妇女参加葬礼，尽管她们的大部分脸被头巾包住了，但中间那位女子眼神中流露出的悲伤清晰可见。

营造悲伤的气氛也是社会工程常用的手段之一，因为它可以激发人们采取某些行动，从而捐款或者提供信息。类似桥段经常出现在电视里的商业广告中：一些无助的孩子，他们缺少爱和关怀，长期生活在清贫的环境里，营养不良，只要你献出一点爱心，就会让他们的脸上浮现笑容。悲伤的神情、满是泪水的脸庞，这些瘦弱的儿童始终会扣紧你的心弦。我说这些并不是意味着商业广告是恶意的社会工程，只是想说明它们使用了一定程度的社会工程，通过触发情绪让目标做出特定反应。

不过恶意的社会工程人员通常会利用人们这种同情心从目标那里获取利益。有一次我走进一家餐馆，无意间听到一位年轻的男子和一群准备走出餐馆的长者的对话。据他描述，他刚从高速下来，车子没油了，他现在急需赶往家中，因为家里的妻子有着9个月的身孕。他刚失业，徒步从高速公路走了一英里过来这边给妻子打电话，他想找这些被他拦住的人借20美元。我听到一半便放慢脚步，装作在打电话，等着看接下来的戏。他继续说着故事，最后加上一句："你把地址给我，我到家便会把20美元的支票寄还给你的，我发誓！"



图5-13 注意她下视的眼神和下垂的上眼睑

这个故事具备了引发他人同情的要素，尤其当他脸上流露出那种对家人的担忧、焦虑和悲伤时。他得到的何止20美元，那三位长者一人给了他20美元。他说了几遍“愿上帝保佑你们”并逐一拥抱了他们，然后说自己进去就打电话给妻子，告知她自己在回去的路上。拥抱后，他们几个就离开了餐厅，心里美滋滋地觉得自己这周又做了一件善事。

几分钟后我在用餐时，发现那个年轻人在吧台和同伴享用各种酒水饮料呢。他能够很好地操控周围人的情绪，将悲伤的故事结合悲痛的表情演绎了出来。

### 5.2.7 快乐

快乐有很多方面，估计单单快乐这一话题就可以讲一章，然而这并不是我关注的。艾克曼博士的书中有很多关于快乐和相近情绪的绝妙观点，里面阐述了这些情绪如何影响自己及身边的其他人。

我在这里想强调的只是快乐的几个方面，最重要的一点便是如何辨别微笑的真伪。识别真假笑容是帮助我们更好地读懂人类表情的重要方面，对社会工程人员来说，这有利于他们掌握如何呈现笑容。

你有没有过这种经历：碰到某个人，他看起来很开心，但是在和他辞别后，你的配偶或者你自己会觉得刚刚这人笑得好假？

你可能并不清楚什么样的笑容才称得上真实，然而脑子里总有种声音告诉你“这家伙在假笑”。18世纪晚期，法国神经学家杜兴·德·布伦（Duchenne de Boulogne）针对笑容做过

一些卓有成效的研究。他将电极附着在试验者的脸上，通过电流产生和微笑一样的肌肉反应。尽管试验者的肌肉和正常微笑时的运动完全一致，德·布伦还是觉得他是在“假笑”。这又是何故呢？

德·布伦指出，当一个人真实地微笑时，会触发颧大肌和眼轮匝肌（眼周的肌肉）两块肌肉，而眼轮匝肌的运动是自发的，不受外力触发，这也就是辨别真假笑容的关键所在。

艾克曼博士与杜兴的研究成果不谋而合。虽然近期的研究表明有些人可以通过训练来触发那块肌肉，但通常情况下，真假的辨明就在于眼睛。真实的笑容是由眯着的眼睛、上扬的双颊和拉起的下眼睑构成的。它由眼及口，牵扯到整个脸部的运动，如图5-14所示。

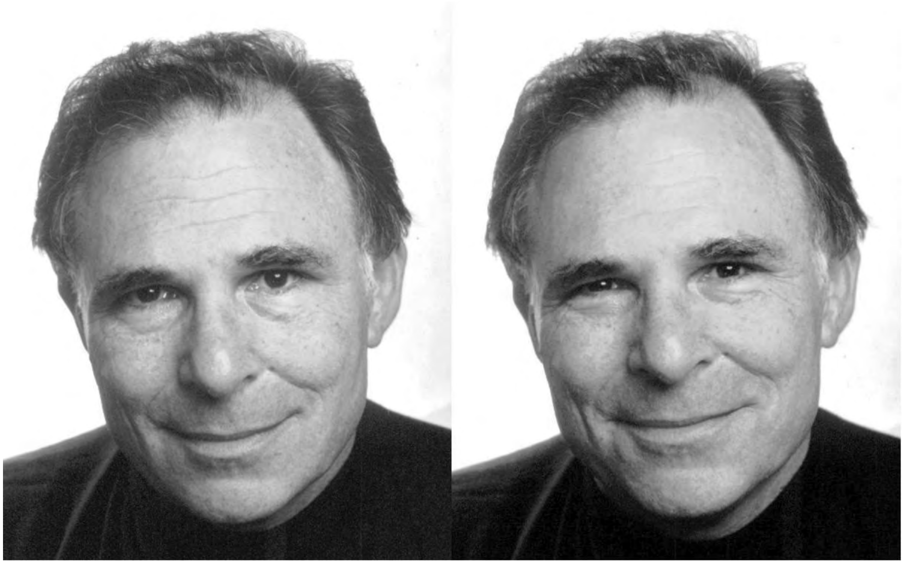


图5-14　艾克曼博士演示的假笑（左图）和真笑（右图）

如果你遮住艾克曼博士的上半部分脸，估计会很难区分笑容的真假。直到看到左右两图中艾克曼博士眼睛的对比，才能区分得出来。

如果一个人对他人展示出发自内心的笑容，在他的感染下其他人也会流露出相同的喜悦并微笑的。注意图5-15中的两个和尚，左边那个和尚展现出了真实的笑容，他是真的开心。你看着图片中的他，自己也会跟着开心起来。

从社会工程的角度来看，知道如何觉察和伪造出以假乱真的笑容是很有价值的。他们竭力想让目标对象放松，从而得到最积极的效果。不管伪装成什么角色（销售人员、教师、心理学家或其他的角色），社会工程人员开启对话的第一步通常是一个微笑。我们的大脑在接收到这个视觉输入后会快速地进行分析并得出结论，对这个微笑真伪的判断直接影响后续的交流。



图5-15 他整张脸都在笑

前文涵盖了很多信息，你可能想知道社会工程人员是如何训练自己，从而不仅能够识别微表情，还能够熟练地运用的。

## 5.2.8 训练自己识别微表情

好莱坞经常会夸大影视剧中角色的能力。例如在热播的电视剧《别对我说谎》（*Lie To Me*）（基于艾克曼博士的研究）中，剧中的主角莱特曼博士（Dr. Lightman）可以毫不费力地读懂他人的微表情，更神奇的是他通常能说出情绪产生的原因。

然而在现实生活中，这一领域中，像艾克曼博士这样的人员所做的大部分工作并非这么轻松，这种研究意味着坐在录好的视频片段前逐帧地进行分析。这样的研究要做好多年，他才能快速注意、识别和分析微表情。20世纪70年代，通过一项专题研究，艾克曼博士发现有些人天生就具有感知并准确分析微表情的能力。

然而具备这种能力的人毕竟是极少数，所以大部分人都需要不断地练习及训练，才能够熟练地展现、读懂并运用微表情。在这里和大家分享一下我的训练方法。我先研究特定微表情的鉴别方法，然后对着镜子参照专家描述的步骤进行模仿。通常我都会拿一张展示这种情绪的照片，对着照片模仿对我大有帮助。

当觉得自己模仿得不错的时候，我便开始专注于酝酿感情、调整细节，直至面部肌肉的运动和情绪能够一致。

然后，我从网上寻找不同的表情图片，试着去揣摩其表达的情绪。接下来试着将新闻或电视节目录下来，以较慢的速度去静音播放，看自己能否准确辨别说话者的情绪，之后再听原版的故事，看自己猜得是否接近原意。这些都是为"实战"做准备。然后我会观察人们之间的交流，尝试识别他们交谈过程中的情绪波动。我不仅会观察那种可以听到谈话内容的对话，也会观察那些无法听到交谈内容的场景。

我之所以没有直接在自己的会话中练习，是因为不用在训练的时候去注意自己的谈吐和话题的接转，这样要更容易些。我只需专注地去阅读面部表情即可，不用被自己其他的感觉所干扰。在有幸见到艾克曼博士之前，我一直是按前文所述的这种方法训练的，见到他之后，他传授给我另外一套方法。当然，还有他的那些著作，里面有解读和重构表情的分步式的教学方式，还有不同情绪所对应表情的照片、新闻中的实际例图等。他的《情绪的解析》以非常专业的方式对此进行了解读，该书非常值得一读。

近几年，艾克曼博士研究并发布了针对微表情的专业训练。在网站www.paulekman.com中，他提供了3种训练模式，从而改变了人们掌握这门强大科学的方式。

针对每一种微表情，艾克曼博士的训练课程都有视频和文本说明。网站用户可以重放每一种表情的形成过程的视频，观察面部运动的每一个细节。一旦学员花了足够多的时间在上面学习并观察这些视频，便可以参加预备测验，检测自己对于微表情的识别达到了何种水平。当学员提交自己的猜测结果后，正确的回答会得到确认，错误的回答会得到纠正。如果需要纠错的话，可以参加额外的学习和培训。

当用户觉得胸有成竹的时候，可以参加正式的测试。最后的考试没有纠错，学员将要辨别时长为1/25秒的微表情，然后必须作出判断，到最后才有总分。

根据学习的成长（效果）曲线，通过这种训练工具训练几年，就能熟练解读微表情了。然而，艾克曼博士和他的同事却警告说：就算你精于解读微表情，仅能解读它也是远远不够的。他们何出此言呢？

演员常用的一种技巧是尝试从过去的记忆和经历中成功找到和想要表达的情绪一样的事件，例如回忆过去的一个快乐瞬间就会产生一个真实的笑容。前文曾提到，如果并不开心，想要刻意装成很开心是很困难的，但是如果你能唤起让自己感到开心的回忆，你的面部肌肉便会依据记忆作出自然的反应。

因此，尽管可以熟练地辨别微表情背后的情绪，却很难读懂每种情绪的触发因子。这种因子无法从科学的角度去阐释。我有一个朋友，在儿时曾经与某人有过一些不愉快的经历，而那个人和我的另外一个好朋友长得非常像。每当我这个朋友来访，她的情绪都会有很大的波动。你可以

从她面部的微表情中读到恐惧、轻蔑和愤怒。她并不是讨厌我那个朋友，而是讨厌那个记忆深处长得和我朋友很像的那个人。

在学习解读微表情时，记住下面这一点很重要。每种表情背后都有一种情绪，然而仅仅通过表情是无从得知该情绪的起因的。当学习微表情达到比较“熟练”的地步时，我感觉自己就像掌握了读心术一般。事实上一定要当心，不要想当然，离“读心”还远着呢。也许你已经精通读懂微表情的方法了，接下来便教你如何把这种技巧与沟通手段、肢体语言以及诱导方式有效地结合起来运用，让你不仅能够明确目标对象的想法，还能够将他们引到你想要的方向。

可能你心中还有一个疑问：“作为社会工程人员，要怎样运用这些技巧呢？”

### 5.2.9 社会工程人员如何运用微表情

研究很让人着迷，背后的心理学原理很神奇，但我们如何将微表情应用于社会工程审计呢？恶意的社会工程人员会怎么利用它呢？ 本小节就是要给出该问题的解答。

本节将讨论两种将微表情运用于社会工程的方法。第一种是使用微表情去诱导或者诱发某种情绪，第二种则是使用微表情识别欺骗。

首先来看第一种方法，使用微表情令目标对象产生相应的情绪反应。近期读过的一篇研究论文改变了我对微表情的认识，令我见识了一个新的研究领域。研究人员李文（Wen Li）、理查德·津巴（Richard E. Zinbarg）、史蒂芬·勃姆（Stephan G. Boehm）和肯·派勒（Ken A. Paller）发起了一项名为“情绪在下意识里的面部表现和性格焦虑带来的影响在神经和行为上的证据”的研究，这项研究改变了微表情在当代科学中的应用。

研究人员在试验者的面部肌肉上连接了几十个迷你心电记录器。这些器件将试验者脸上和头部肌肉的运动记录下来。然后，他们为试验者播放多段视频，视频中包括1/25秒时长、一闪而过的微表情。李文等人发现，几乎在所有情况下，试验者的肌肉运动会重复视频中嵌入的微表情。如果是恐惧或者悲伤，试验者的面部肌肉会产生相应的情绪。问及试验者的感受时，他们表示和视频中嵌入的情绪是一致的。

对我来说，这项开创性的试验表明，人们可以通过一些情绪上的微妙暗示操纵他人达到特定的情绪状态。我从安全角度开始了这方面的研究，并称之为“神经语言入侵”，主要原因在于它将微表情与神经语言程序学（下一节讨论）结合起来，在目标心中产生某种情绪状态。

设想这样的场景：一名社会工程人员要进入一家公司，目的是让前台将带有恶意程序的U盘插入电脑。他的伪装是和人力资源经理约好了过来面试，但路上不小心将咖啡洒到最后一份简历上了。他真的需要这份工作，也需要前台的帮助。前台会帮他重新打印一份简历吗？

这一伪装在引起对方共鸣方面相当有效，我之前就利用它获得过成功。然而，如果社会工程

人员不能很好地控制自己的情绪，就可能会表现出恐惧，从而引发紧张。这种恐惧可能会转化为前台人员的紧张，最终导致自己的请求被拒或者行动失败。而如果他能够控制好自己的情绪，让自己表现出微妙的伤心的微表情，就会轻易激起同情，而他的请求也就很容易获得应允。

回顾前面讨论的广告，它鼓励市民“每天捐赠一美元，养活一名贫困儿童”。在要求捐款之前，在显示电话号码和网址之前，在告诉你接受信用卡捐助之前，电视屏幕上会展示很多伤心孩子的照片。这些亟需救助的痛苦的孩子的照片会引发你的怜悯，促使你做出捐助的行为。

这些广告对每个人都奏效吗？当然不是。然而，虽然不是每个人都捐，但它会影响几乎所有人的情绪状态。这也是社会工程人员充分使用微表情的方式。学习展现这些带有暗示性的微表情，会引起目标对象大脑中的神经元反映相同的情绪状态，使他更愿意遵照你的要求去行动。

这种微表情使用方式也被用于恶意的目的，所以我想花点时间谈论如何防御这种攻击（第9章也会介绍这方面内容）。要注意微表情的使用方式，但这并不意味着需要将公司里的每个人都培训成微表情专家。其真正的含义是必须加强良好的安全意识培训。即使对方设计出来的请求让你很有欲望去帮助、拯救或照顾，也要确保首先贯彻安全策略。可以简单地说一句：“对不起，我们的电脑不允许接入外来U盘。不过，离这里两英里处有一家联邦快递金考快印店。你可以去那里重新打印简历。需要我告诉史密斯女士你会晚到几分钟吗？”

在这种情况下，如此的婉言拒绝不仅能够让社会工程人员的计划泡汤，也会让目标觉得自己帮助了他人。

想要发挥微表情的作用，有时也需要和人类行为的其他方面相结合。第二种方法——识别欺骗，将会告诉你如何做到这一点。作为社会工程，使用微表情的第二个方法的目的在于识破骗局。如果你可以通过问一个问题，知道他人的回答是否真实，会不会感觉很好？这也是专家们热烈讨论的话题，有些专家认为通过眼神、肢体语言、面部表情或结合以上3点就可以识别真伪。然而有些专家却不以为然，还有一些专家认为这可以作为一门精准的科学来应用。

尽管各方的观点都有一定的事实论据，但是如何运用微表情来识别骗局呢？

要回答这个问题，思维就不能被微表情所局限，因为通贯本节的内容，微表情都是以情绪和情绪的各种反应为基础的。因此阅读本节时请铭记这一点，本节还分析了一些因果关系。

以下4种反应可以帮助你识别目标的诡计。

- 矛盾
- 犹豫
- 行为的变化
- 手势

下面将详细地讨论这些反应。

### 1. 矛盾

“矛盾”这种情况处理起来特别棘手，因为它们可能确实会在现实中发生。我就经常会忘记一些事情的细节，而我的妻子总会迅速地予以补充。在得到一些提示之后，我通常就能记起完整的故事。这并不意味着我在故事或对话的一开始就撒谎，而是在一开始就整件事发表评论的时候，我并不能记清每个细节，或者是我认为自己记得，而实际上并不记得。即便我“想起”了具体细节，也不是实际发生的情况，而可能是我自己认为的事实。

在评估是否将矛盾作为说谎的线索时，对这种无意的“谎言”进行考虑显得尤为重要。一旦发现矛盾的情况，你所要做的应该是挖掘更多的信息。就矛盾之处进行询问，注意观察他的微表情变化，也有助于对真实情况作出判断。

例如，假设你伪装成上门拜访的销售人员，打算通过给他们的CEO派发特价CD的方式进入公司内部。你事先了解到这位CEO比较关注某慈善机构，所以伪装的角色与此有关。当你走进大堂时，前台接待却说：“对不起，他不在，你把东西留在我这里就可以了。”

你知道如果就这样将CD留给她，那么其中植入的恶意程序很可能永远不会发挥作用。而且你觉得他在公司，因为看到他的车就在停车场，而且今天是工作日。综合这些事实，又不希望前台难堪，你说道：“哦，他不在吗？我前几天给他打电话询问什么时候可以过来拜访，他说今天可以。我记错日子了吗？”

如果你出对了牌且表情真诚，可能会有以下两种结果。

- 她可能会镇定地告诉你说：“对不起，他不在公司。”
- 她可能会前后矛盾（这可能是她之前没有说实话的一个线索）：“让我再确认一下。”

什么？她从坚决地声称“他不在公司”转成“让我确认一下”。这一前后矛盾足以提醒你应该挖掘更多的信息。她说这句话时有哪些微表情？她有没有因为撒谎而感到羞耻或难过？她有因谎言被拆穿而生气吗？她为所犯的错误感到尴尬或困惑吗？你不能想当然地断定她在撒谎，因为也许她是真的不知道，在你辩驳的时候她才决定去确认清楚。

在她核实之后，必要的话可以挖得更深一些，探查更多信息，以试探事实真相。你可以重申：“可能是我记错日子了。”通过仔细观察她的面部表情能够精准地判定她是否在撒谎。

第一轮交谈下来，如果你在她脸上看到了愤怒的特征，继续刨根问底可能会使她更加愤怒和尴尬，导致会话的终止。这时候，你可能要这样问：“如果史密斯先生现在不在，可能真是我记错会面的时间了，那么什么时间过来能见到他呢？什么时间最合适？”

这种类型的问题可以令她挽回面子，还给了你解读她面部表情的另一次机会。如果你注意到她的脸上并没有流露出愤怒，而是有点难过或者尴尬，你可以回之以同情和理解，让她能够敞开心扉。“我敢发誓，他和我约好今天见面。可是我的记性很差，我老婆甚至说我有老年痴呆症。

我买了部智能手机，如果知道怎么设定的话，可能会对我的记忆有所帮助。我也不想添麻烦，只是我什么时候能过来把东西给他呢？我一定得亲自交到他手上。”

留心观察细小的矛盾之处，因为它们可能是欺骗的关键标识，能够帮你迈进门槛。

#### 2. 犹豫

和矛盾类似，你也可以通过他人的犹豫识别潜在的谎言。如果你问一个他本应即刻回答的问题，而他却犹豫不决，可能是他在利用迟疑的这段时间来编造答案。

例如，当妻子问我新买的电子设备多少钱时，她知道我肯定记得。如果此时犹豫的话，往往意味着我在盘算是否要如实回答，当然也有可能我确实在回忆价格。

当从学校提供的成长报告中发现儿子有X天缺席，而我印象中只有2~3天时，我问他其余那些天是怎么回事。如果他的回答是：“爸爸，还记得有一次我们预约了医生看病，然后你让我在家休息一天，还帮着你一起做项目吗？”这很有可能是实话，因为他反应够快，并且有事实作为支撑。不过，如果他犹豫了一下说：“哦，我不知道，可能报告搞错了。”此时要注意观察他说这句话时的微表情。是因为被抓而觉得愤怒？还是为想象的惩罚感到难过？无论是哪种，我都应该深入调查那些天他到底在哪里。

另一种需要注意的众所周知的犹豫战术就是重复你所提出的问题，好像是对问题进行确认，这样的话就有时间来编造答案。仅仅通过犹豫来识别欺骗是不科学的，但它可以作为一个很好的信号源。有些人只是习惯于谨言慎行。我是纽约人，语速比较快。如果有人说话比我慢，并不一定都是在撒谎。你必须能够运用微表情去辨别他是真正说话慢，还是在试图编造答案。

如果他反馈的情绪和提出的问题不匹配，可能就值得推敲了。

#### 3. 行为的变化

在交谈的过程中，每次谈到特定的话题，目标的行为都会发生变化。也许是表情的变化，或者是坐姿的改变，抑或是明显的犹豫。所有这些动作都具有欺骗的特征。虽然这些行为不一定等同于欺骗，但是你应该在不引起怀疑的情况下，继续深入这一话题。这些行为可能是一种信号，对方在利用时间的延迟来编造故事、回忆事实，或者决定是否要向你透露实情。

#### 4. 手势

人们经常会用手势来描述场景。例如，用双手去比划某件物品的大小、某种物体运行的快慢，或者某件事被提及的次数等。许多专业人士认为，人在撒谎时会频繁地触摸或者摩擦自己的脸。从心理学的角度来看，这两者之间有一定的联系。网址www.examiner.com/mental-health-in-new-orleans/detecting-deception-using-body-language-and-verbal-cues-to-detect-lies中给出了一些心理学家和肢体语言专家关于检测欺骗的线索和暗示的讨论。

交谈过程中，留心观察手势的幅度、频率以及时长的变化很重要。不仅如此，做不同手势时的面部表情也要格外注意。

当你发现欺骗行为时，制定一个应对方案非常重要，也是个不错的做法。前面提到的场景中，当前台说CEO不在公司时，如果你当面指出她在撒谎，很可能会令场面陷入紧张状态，使她倍感尴尬，葬送一切可能成功的机会。如果你伪装的是权威人士，例如经理或者部门主管，抓住对方说谎可能会对你有利，因为你可以通过“原谅”对方让他欠你一个人情。但在同样的情形下，如果你的职位（比如是非管理岗位的秘书、接待员或者销售人员）低于目标人物，使用这种策略是很危险的。这种权威性的行为不适合非管理职位的伪装者。

综上所述，作为一名社会工程审计人员，必须学会观察他人的微表情，判断对方说的是实情还是谎言，并确定自己是否在按照想要的方式影响目标。在某些情况下，你甚至可以利用特定的表情操控目标的情绪状态。

记住，仅仅依靠微表情是不足以判断情绪产生的原因的。例如，即便能判断出目标是生气还是伤心，你也很难知悉个中缘由。在运用微表情的时候，需要细心谨慎地考虑各种因素，才能得出产生某种情绪的最可能的原因。

恶意社会工程人员会采用本节讨论的微表情技术，但是他们的目的和做审计的社会工程人员完全不同。他们往往不会顾及对目标的后续影响。如果破坏一个人的信仰体系、引发目标心理不稳定或者让目标失去工作会给他们带来利益，他们会毫不犹豫地去做。

前面章节提到过纽约“9・11恐怖袭击事件”之后发生的一些骗局。有些人不顾给他人造成的伤害，利用人们的同情心和灾难骗钱。许多人从阴影中走了出来，声称在这次袭击中失去了家人。这些充满恶意的人接受了捐助的金钱、礼物和同情，甚至引起了媒体的关注，最终却被人们发现他们的故事都是编造的。

恶意社会工程人员会花很多时间研究人，分析人们会因为什么上钩。这些知识会帮助他们找到易受攻击的目标。

本节谈及的微表情还较为浅显，该领域的专业著作称得上汗牛充栋。寻求培训，熟练解读和运用微表情，可以明显提升你与他人沟通的能力。此外，精通微表情会提高你的能力，从而在审计活动中获得成功。

## 5.3 神经语言程序学

神经语言程序学（NLP）研究的是人类思考和体验世界的结构。然而，由于NLP结构本身并不具有精确性或者符合某种统计公式，所以引起了很多的争议。很多科学家因此针对NLP的基本原则展开了讨论或辩论，但是NLP结构确实可以推导出运行框架模型。从这些模型中，又开发出

了可以迅速而有效地改变或限制人类思想、行为和信仰的技术。

根据维基百科（来源：《牛津英语词典》）的描述，神经语言程序学是“一种人际沟通模型，主要关注成功的行为模式和内在的主观经验（尤其是思想模式）之间的关系”，和“一种非传统的治疗系统，旨在教育人们要有自我意识和进行有效的沟通，并改变他们的心理和情绪行为的模式”。

因为这远非一本自助式图书，所以书中的内容虽然有助于你改变自己根深蒂固的思维模式和习惯，但是其重点还是如何运用NLP来理解和操纵周围的人。

如果不熟悉NLP，你的第一反应可能是找一台计算机，在谷歌中进行搜索。希望你暂时不要这样做。与社会工程学类似，你会首先发现很多看起来很不真实的视频和演示，例如视频中某人触摸另一个人的肩膀，就改变了这个人的大脑思维模式，以至于认为棕色是白色或其他颜色。这些视频使得NLP很神秘。对于那些持怀疑态度的人，这些类型的视频会让他们不相信NLP。

下面将NLP分解成几个部分。下一节是NLP历史的简短介绍，它有助于你理解NLP不是源于街头艺人，而是具有深刻的心理学渊源。

### 5.3.1　神经语言程序学的历史

神经语言程序学起源于20世纪70年代，由理查德·班德勒（Richard Bandler）和约翰·葛瑞德（John Grinder）在格雷戈里·贝特森（Gregory Bateson）的指导下提出。其根源是班德勒和葛瑞德对他们那个时代的一些最成功的治疗师的研究。

从这个初始研究起步，他们提出了NLP“准则”的概念。这一早期研究使元模型得到发展，元模型认为通过语言模式的使用能够对变化产生影响。

班德勒和葛瑞德当时都是美国加州大学的学生，他们使用研究中的原理，开发出了一种称为“元模型”的治疗模式。基于此模型的几本书出版后，他们开始细化其核心原理，最终形成了我们今天所说的NLP。这包括心锚（anchoring）、快速心态转变法（swish pattern）、换框法（reframing）、转变信念（belief change）、嵌套循环（nesting loop）、串联状态（chaining state）和次感元（submodality）的应用。

在拿到心理学学位之后，班德勒和葛瑞德开始举办研讨会和群体实践，这为他们提供了训练和测试新发现的模式的场所，同时允许他们向参与者传授技巧。在此期间，一群具有创新思维的学生和心理治疗师聚集在他们周围，为NLP学术作出了宝贵的贡献，使得NLP更加完善。

近年来，NLP成为了管理者的新流行语，使得这方面的培训人员、课程和专家群体快速增加。在没有管理机构的情况下，每个人都想学习控制他人、在撒谎时不会被拆穿，或者解决自己的心理问题，所以该领域不断发展。从业者没有执照，所以每个群组都教授他们自己的NLP形式和概念，并作为专家颁发自己的证书。所有这一切使得NLP给人们留下了糟糕的印象。

抛开其坚实的历史因素，NLP的核心基础能够提高社会工程人员的能力。下一节将讨论NLP的一些核心准则，以便于你进行更深入的分析。

## 5.3.2 神经语言程序学的准则

20世纪70年代初，NLP就拥有一组学习和调查的准则，并由此产生了第一批书籍和“神经语言程序学”这一术语。随着时间的推移，约翰·葛瑞德和其他人在NLP领域不断作出贡献。“NLP新准则”是NLP发展的道德和美学框架。

### 1. NLP新准则

NLP的原始思想产生于20世纪70年代。随着时间的推移，约翰·葛瑞德开始认识到必须更新许多老的准则，以适应新的时代。他开始与格雷戈里·贝特森和朱迪思·德洛齐耶（Judith DeLozier）一起研究“新准则”，新准则更加关注人们思维和信念的产生以及信念的转变。扩展认识的学习技术、克服旧的思维模式以及改变习惯都有助于带来自我改变。

新准则聚焦于状态、意识和无意识之间的关系及知觉过滤等关键概念，所有这些都指向人们的思维状态及其对那些状态的感知。这些新概念旨在推动和发展NLP，帮助NLP实践人员以新的方式思考NLP。新准则的许多基本原则现在已成为标准NLP课件的一部分。这一新准则可以通过阅读葛瑞德和德洛齐耶合著的《路途海龟：天才的条件》（*Turtles All the Way Down*）一书来充分地理解。该书是根据其研讨会“个人天赋的先决条件” 的内容汇编而成的。

从本质上讲，新准则指出人们必须通过潜意识思维做出改变，新的行为必须符合其原始的积极意向，而且改变必须发生于思维状态内部，而不仅仅是行为层面。这一新准则表明NLP如何能够造成一个人思想上的严肃而巨大的改变。

对社会工程来说这是一个关键的概念，因为在调查和分析新准则时，你会发现如何利用它来操纵他人。不过在此之前，你需要了解新准则所使用的脚本。

### 2. 新准则的脚本

人们往往有共同的问题，所以新准则中开发出一组脚本来帮助治疗师在实践中使用NLP。这些脚本引导参与者进行一系列的思考，这些思考有助于引导人们取得预期的结果。关于NLP脚本有几本很好的书，我强烈推荐《NLP技术大全：神经语言程序学的200+模式与策略》（*The Big Book of NLP Techniques: 200+ Patterns & Strategies of Neuro Linguistic Programming*）。

脚本的一个例子是如何通过让人们谈论自己的梦想以提高销售额的大纲。一旦让人们谈论起具体的目标或愿望，你就可以将产品或服务定位成实现该目标的一个必要条件。通过将产品与人们的需求联系起来，就可以让产品带来销售额。

如果花时间到谷歌上搜索这里提供的大量信息，你会发现NLP本身就具有生命力。在学习

NLP时可以采取多种角度和路径。尽管有关NLP的信息和内容很多，但问题仍旧是社会工程人员应该如何使用NLP呢？

### 5.3.3　社会工程人员如何应用NLP

许多NLP脚本和原则往往倾向于催眠和类似的方法。即使不采用催眠目标的方法，作为社会工程人员，你也可以使用NLP中的许多原则。例如，NLP可以教你如何运用声音、语言和精选的词汇来引导人们按照你设想的去做。

#### 1. NLP之于语音语调

你可以用声音向人们注入命令，就像用代码向SQL数据库中注入指令一样。你说事情的方式就是注入发生的地方，注入的时刻包括在常规对话框架中。有时，如何说比说什么更加重要。

NLP提倡使用嵌入式命令影响目标以某种方式进行思考或采取某种行动。此外，通过变换语调强调句子中的某些词语，使得人们的潜意识将重点放在那些词语上。举例如下。

如果要问“你不同意？”，不要像常规问题那样，在问题的结尾——“同意”处使用升调，而要使用降调，使得该问题更像一个命令。

我知道的另一个行之有效的例子大致是这样：“我的客户通常会按照我说的去做。你要开始吗？”这句话通常和其他语句结合在一起，使得它更像一个命令语句。

下面有更多这样的技巧，但仅此技巧就可以改变你与他人互动的方式，NLP详述了该技巧的基本原则。

#### 2. NLP之于句型结构

在英语中，人们在句子结尾使用的音调，会表明正在说的是一个问题、陈述还是命令。句尾音调上扬说明是一个问题，语音保持一致则为陈述句，而语音下降则类似于命令。

在接下来的几段中，**加粗字体**表示降低你的语音语调下降（或上扬）。

试试这个练习。当你问一个问题时，例如“那是你的狗吗？”，你的声音在句子结尾会上扬。然而，你可以通过改变句子中的语音下降点（不是在句末）在该句中嵌入微妙的命令。这里有几个简单的命令供大家练习，请注意如何在句子中注入命令。

> “记得去年圣诞节**你的房间**打扫得多**干净吗**？”嵌入的命令是“你的房间”和“干净”，其中包括了到过去快乐时光的一个切换。这是一个愉快、无痛注入的例子。
>
> “**现在**就买，立刻**受益**！”这句从低调开始，然后上升到正常音调，在句末“受益”处音调下沉。
>
> “**我公司**在咨询界的**地位越高，像你这样的优秀人才**我们遇到得越多。”语句中植入

了一个愉快的评论“我公司地位越高”，增加了你被公司聘用的机会，部分原因是该句玩了把文字游戏[英语中“地位越高”（higher）和“聘用”（hire）的发音相似，因而听者潜意识中会听到“**聘用我们公司**”]。

从社会工程的角度来看，你可以在通过电话进行审计时，精心构造语句，以最大限度地提高成功的可能性，举例如下。

“我是技术支持部门的拉里，我们为代理**设定了**新密码。**您**的新**密码**是……”

下面是在成功的社会工程中运用语音技术的一些技巧。

- **实践**　必须不断练习这种说话方式，这样就不会听起来像刚刚步入青春期的十几岁的男孩。语调的上升和下降不能太做作，必须用得很微妙。
- **周密的语句结构**　构思最有利于完成任务的句子，不要指望一句话就能起作用。类似“请让我现在进入服务器机房”的指令可能行不通，但你可以运用语音语调上的技巧，使目标更易于接受这一想法。
- **保持现实**　不要指望通过说几句话就能让目标言听计从。运用这些技巧的目的是让目标进入某种思维框架，使你更容易得偿所愿。

有一种技术称为终极声音，如果掌握了，它会产生非常强大的效果。我曾经在播客上采访过一位具有这种天赋的NLP实践者。当他说话时，你似乎不可能与其发生争执。他的谈话具有如此的控制力和技巧，我的头脑中根本不会产生有分歧的想法。如何才能掌握这门技术呢？

### 3. 在社会工程中使用终极声音

人们能够掌握终极声音，但需要大量的练习。在正常的谈话中嵌入指令是一项一经掌握就很有实用价值的技巧。终极声音是一种在人们不知道的情况下注入指令的能力，在新人进行尝试时似乎很造作，只有经过足够的练习才能达到自然的程度。

催眠经常会使用这种技术，举例如下。

“当内心**平静**时，你会感到自己很**放松**。”

这一标准的治疗短语适用于你喜欢的任何命令。格外强调单词中发出的元音，例如：“你……会放松……[①]。”

NLP大系网站（www.planetnlp.com/）提供了3个练习，你可以通过它们掌握这项技能。

(1) 让你的声音具有动感　将手放在鼻子上说“鼻子”。将注意力集中在鼻子上重复说“鼻子”，直到能感觉到鼻子在振动。现在做同样的练习，将手放在喉咙上说“喉咙”。同样将手放在胸部说“胸部”。坚持练习，直到你可以真正感受到各个部位的振动。请注意每个单词

① 原文是“yooouurseeelf reelaaxiing”。——译者注

发声的不同。

(2) 发挥你的极限　从一个高音符开始，说“ar”（类似字母r的发音）。保持嘴巴张开，让音符持续降低，直到你的呼吸耗尽。

重复练习10遍。

然后开始一个低音训练，说“ou”（就像少了字母y的单词you），使音符持续上升，直到不能再高为止。

重复练习10遍。

(3) 共鸣　正确使用你的声音，必须在面罩处产生共鸣，也就是围绕鼻子和嘴唇的面部区域。

练习共鸣的方式有两种。

- 哼哼你感到最舒服的音调。在找到你的音调后，然后哼出“嗯”的声音，随后立刻说出“好了”[①]。重复数次，然后再尝试说出“现在”、“一”、“二”和“三”。
- 发出哼哼声，然后让你的嘴唇振动。尝试像鸽子一样发声。让音调时而上升时而下降。如果下巴或脸部有些紧张的话，会很难持续。按照正确的方法做几分钟，你就会开始觉得脸部麻木了。

这些方法练习几分钟之后，你会发现自己的声音听起来更轻快。如果你认为难以察觉到，将声音录下来并做前后比对。

改善的最好办法就是每天花5分钟左右将这些练习都做一遍。

实践有助于你学会控制这个发声技巧。例如，一般来说，我是一个声音响亮的人。我似乎没有窃窃私语的能力。如果要控制我的语调、音调和声高，就需要不断的实践练习。通过这些简单的声音练习，能够帮助你控制这些语音特征。

当想在说出的句子中包含一个隐藏的命令时，你要降低语调，通过细微的变化使目标意识不到其中命令的成分。否则你会提醒对方的潜意识，让他觉得什么地方出了问题。如果出现这种情况，他会觉察你的企图，让你难以成功。

和社会工程的大多数技能一样，如果一门技巧不是与生俱来的，则练习是必不可少的。在审计中使用该语音技巧之前，应该首先在家人和朋友身上进行尝试。

从个人经验来看，第一次使用终极语音技术时，我设定的目标是将命令嵌入到问题中。这个目标花了一段时间才得以实现，但我是从较简单的事情开始的，如：

> “亲爱的，今晚**你想吃**什么？**牛排**还是别的东西？”

---

① 原文是“Ready”。——译者注

最后，社会工程人员在学习NLP时需要关注3件事情。

- **音调**。如前所述，声音的音调以及将重音放在某些特定的词语上能够改变整个句子的含义。通过使用音调和重音，可以在目标的潜意识思维中嵌入命令，使得目标对建议采取更加开放的态度。
- **审慎地选择用词**。学习选择能够产生最大影响的词语。对于想要目标积极思考的问题选择积极的词语，对于那些不需要目标想太多的事情选择消极的词语。这项技术还可以帮助社会工程人员让目标更加顺从。
- **创建一个可用于当面或电话社会工程审计的命令语句列表**。将这些命令语句写出来并不断练习，这样才能在需要的时候即时回忆并应用上。

最重要的是练习。控制语调、审慎选择用词并且注意如何表达，这些事情做起来并不容易。练习能够使它们成为你的第二天性。

NLP是一个具有强大力量的主题，很像微表情，本节只触及皮毛。一旦你开始掌握NLP中的技巧和识别面部表情的能力，从逻辑上来讲，下一步就是在与目标交互的时候使用这些工具。接下来，本章会分析专业审讯人员所使用的相同的战术。

## 5.4 采访和审讯

**情景一** 突然，门被猛地摔开了，犯人明显紧张起来。“坏情绪”队长走了过来，拎起犯人的衣领，一耳光将其扇到墙上。然后凑近他的脸，恶狠狠地说：“把我想知道的通通告诉我，否则有你好受的！”

**情景二** 坏人被绑在椅子上，半小时前已被打得满身伤痕。审讯者抓起一把闪亮的钳子在他面前晃：“你必须立刻说出……”

**情景三** 嫌疑人直坐在椅子上，两名警察进入审讯室。他们静静地走到桌子前，把标有“证据”的文件放在桌上。在坐下来之前，他们问道：“来点咖啡、苏打水，还是别的？”

在打开冰镇苏打汽水的同时，一位警官说道：“感谢你今天过来协助我们……”

上述3个场景哪一个是现实生活中的审讯？如果你猜是第3个，答对了。这是一个真实审讯的常规模式。前两个场景在好莱坞的电影和电视剧中出现过很多次，以至于我们当中的很多人可能认为审讯就是这样的。除了战争时期和未禁止使用酷刑的国家，第3个场景极有可能是大多数审讯开始的方式。

社会工程人员很少会碰到目标对象在房间里等着你问话的情形。考虑到这一点，你可能会问，如何将专业审讯人员和采访者所使用的技术运用到社会工程中去呢？

在深入探讨这个问题之前，我们首先弄清楚审讯和采访之间的差异。下表列出了两者之间的一些差异，但这个话题有许多不同的角度、观点和意见，所以可能还有很多差异没有列示在下表中。

| 采　访 | 审　讯 |
|---|---|
| 目标对象说话，你倾听 | 你述说被审讯者之前的陈述 |
| 目标对象引导谈话的方向，你重申他的叙述并倾听，同时运用NLP技术 | 你主导审讯的方向，运用NLP技术 |
| 无控告 | 有指控 |
| 性质温和 | 性质强硬 |
| 目标对象处，目标处于放松的状态 | 审讯室，被审者很紧张 |
| 你收集信息（人物、事件、时间、地点、原因及方式） | 如果你透漏一点特定信息，会得到更为详尽的细节 |
| 调研初期 | 最终提问环节 |

采访和审讯之间的主要区别在于，采访中目标在身体和心理上都处于舒适的状态，而审讯的目的则是通过审讯的场所和所提问题让目标感到不适来向其施压，从而使其老实交代。

审讯是一门可以通过经验掌握的艺术。要想成为优秀的审讯者，社会工程的很多技术都大有用武之地。诱导（见第3章）、解读人们的表情和手势及洞悉人类的行为都有助于你成为一名了不起的审讯者。

采访是一项很有用的技能，但只要能熟练运用"诱导"，你就已经可以驾驭采访了。

审讯原则被成功的社会工程人员广泛运用。使目标处于身心不适的状态，这样会使信息收集变得更容易，大多数的社会工程人员都愿意花费大量时间来学习这门技术。

### 5.4.1　专业的审讯技巧

在进行采访或审讯之前，社会工程人员都需要完成充分的信息收集工作。你必须获得尽可能多的关于目标、目标公司以及当前状况的信息，而且信息要尽可能详细。你必须知道如何接近目标，想好要说什么，并提前构思好和他打交道的方式。仔细观察周围的环境以及在初步接近和交谈中目标的任何变化。

新手在采访和审讯过程中经常会犯的一个错误就是，总是假设所有的行为改变都有重大的意义。目标对象交叉双臂不一定意味着不想交流，他可能只是觉得有点冷、有腋臭，或者因为你的问题而倍感压力。

不要单单留意一个动作，而要留意一连串的动作。例如，目标交叉双臂，将头转向一边，并把双脚平放在地板上。这是一个封闭的人，换句话说，其身体语言表明他不想泄露任何信息或者

不想再合作，即交流的大门已关闭。一系列的变化是最需要留意的，所以要注意变化发生时正在讨论的话题。

当采访或审问开始时，需要留意目标人物在下列各方面所产生的变化。

- **身体姿势**　直立、瘫倒、倾斜
- **脸色**　苍白、红、白、变化
- **头的位置**　昂首、倾斜、往前/往后
- **眼睛**　方向、睁开的状态
- **手/脚**　动作、位置、颜色
- **口/唇**　位置、颜色、张开/闭合
- **主要感觉**　视觉、听觉、活力、感觉
- **声音**　音高、速率、变化
- **词语**　短、长、音节的数量、功能障碍、停顿

变化可以表明需要更加留意一个或一系列问题。例如，当你询问“请问总经理在吗？我想把这个信息给他看一下”时，对方的身体姿势由原本很放松的状态变成防御状态——身体转向一边，眼睛避免与你对视——这可能是一个很好的迹象，说明他将要说谎，通过进一步的挖掘你可能知道这件事情的真实情况。

尤其要注意目标的措辞。在采访或审讯过程中，要特别注意目标的声音和他回答问题的方式。当你问一个问题时，他多久才回答呢？如果答案脱口而出的话，说明这个答案是预先练习过的。如果思考太久，可能他在瞎编一个答案。响应时间因人而异，因而你必须确定对不同的人来说到底什么样才是“自然的”。

确定目标的自然状态（这是基准），在社会工程中并不是小事，而且必须很快确定。敏锐的观察是成功应用该技巧的关键。一种确定基准的方法就是询问需要对方大脑的不同区域来思考的问题。审讯者问一些没有威胁性的问题，一些需要简单记忆而另外一些需要创造性思维。然后寻找激活他大脑记忆中心的外在表现，如微表情或身体语言暗示。

另一个需要留意的地方是动词时态和代词使用的变化。如果从过去时切换成将来时，表明这些地方需要你进一步调查。切换时态可能表明欺骗。当目标切换时态时，他们可能是在编造一个答案，或者在回忆之前的说法来编造一个答案，进一步询问也可以揭示真相。其他需要注意的地方是音调的变化（在压力之下越来越高吗？）和语速的变化。

不必想着一下子学完这一切。在聆听和观察的时候多加练习，不假思索地快速判断就会变得容易得多。

专业的审讯由许多部分组成。下面将逐一讨论各个部分，并且会介绍社会工程人员如何运用这些技巧。

### 1. 正面交锋

在执法过程中，正面交锋并不意味着任何积极和良好的信息。相反，它意味着警官告诉嫌疑人他就是那个犯下罪行的人。换句话说，这个警官正在做出强烈的指控。但在社会工程审计中，你已经确定了想要目标做的事情，现在你打算告诉他（也许使用前面提到的NLP技巧），他得做你要求的事情。

在面对目标时，你的目的是让他立刻按照你设想的去做。例如，一名社会工程人员走向前台，并问道："总裁先生在吗？我和他有一个约会。"或者，使用正面交锋的角度来说："我来找你们总裁，11点钟我们有个会要开。"注意第2个例子中肯定地声明会议已经按照预期安排好，而且你说话的方式确定会议一定会如期开始。

### 2. 主题延伸

在警察审问时，"主题延伸"指的是审讯者假定一个故事场景来推断为何嫌疑人会实施犯罪。在审讯期间那个故事会多次传递给嫌疑人。"所以他的辱骂激怒了你，你便抓住管子，开始打他车的挡风玻璃。"当警官陈述故事时，他或他的拍档会观察嫌疑人的肢体语言和微表情，看是否有任何线索可以表明案发经过和刚刚的叙述有吻合的地方。

虽然社会工程人员可以使用这种方法，但我也想说明一下，从社会工程的角度来说，主题延伸必须是从目标的眼中来看你的伪装。"技术支持人员"、"经理"或"同事"看起来什么样？会说什么？做什么？他又该如何做事呢？

社会工程人员的主题延伸，可以理解为你展示的辅助性证据直接支持所描述的主题。无论是通过电话还是面对面，在接触目标的时候都会涉及某种伪装。这个伪装当然会支持你描述的故事情节或主题。审讯的这部分技巧正是为伪装提供理由或支撑的地方（可重温一下第4章中关于伪装的内容）。

例如在一次审计中，我的伪装很简单——扮演成一个普通的雇员。手里拿着垃圾桶中找到的行业杂志，我跟着几个雇员穿过大门和保安。当走近保安时，我开始与其中一个员工简单聊了聊杂志上的文章。我的所有行为都有助于主题延伸。目的在于给那些通常会阻止你的人一个不去那样做的理由。

越融入环境，越不容易被识破，也就越容易麻痹保安等人，使你顺利进去。

### 3. 应对拒绝和反对

无论是通过电话还是面对面，如果对方不允许你进入某地或者拒绝透露你想要获得的信息，你要采取什么行动呢？我一般将这些谈话称为搪塞。人们总是对促销人员这样说："我不感兴趣。""我现在没有时间。""我要走了……"

无论目标抛出什么话来搪塞，你必须有应对计划，以克服和处理这种"拒绝访问"。如果觉

得情况不妙，我会先发制人，让对方难以反对。

从事销售工作的时候，我曾与托尼一起挨家推销，他的本事是敲开门后介绍自己，紧接着就说："我知道你可能要说不感兴趣，但在此之前，请先回答我一个问题，即你的5分钟值500美元吗？"

这时候，人们不太可能说："我不感兴趣。"通过降低被拒的几率并跟进一个问题，托尼能够让目标在反对之外思考一些别的东西。

在社会工程过程中，你不能径直走向保安说"我知道你不想让陌生人进门，但……"，因为这会引起太多的怀疑。对于社会工程人员来说，运行克服反对的方法要复杂得多。

你要预想可能会出现什么反对情况，仔细组织你的主题、故事、着装、人物，从而预先消除那些反对。然而当反对声出现时，还必须有一个很好的回应。你不能只是逃出门或挂断电话。恰当的退出策略有助于你之后发起反击。

退出策略可以很简单，比如："好吧，女士，很遗憾你不能让我见史密斯先生。我知道他也会非常失望的，因为他希望我来，不过我会给他打电话再预约。"

#### 4. 保持目标注意力集中

如果前期的社会工程工作很顺利，你和对象开始面对面接触时，目标可能开始考虑如果不允许你进入、拿走文件或者满足你的其他要求会产生什么样的后果。你需要克服内在的恐惧，镇定自若地按照预定的目标驱动对方。

也许是类似这样的短短几句话："谢谢你的帮助。对于这次面谈，我太紧张了，结果把日程安排记错了。我希望人力资源部经理的办公室比这里要暖和些。"等目标回复后再继续说："非常感谢你的帮助。她什么时候回来呢？这样我就可以打个电话另外预约了。"

#### 5. 展示其他途径

当你在社会工程审计过程中盘问一个目标时，你的第一方案不一定会奏效，所以提前准备好能够达到近似效果的替代方案不失为一个好主意。

也许你已经使出浑身解数去接近前台莎莉，想让她允许你进去见史密斯先生。眼看着所有策略都将宣告失败，你就要被拒之门外了，此时你应该启动准备好的替代方案，例如："莎莉，我很欣赏你的这种工作风格，确保一切会面必须首先经过预约。只是我不知道何时才能再经过这里。我可以把这张资料光盘留给史密斯先生吗？这样我明天可以打电话问问他是否能安排会面。"

在反复练习并能够快速运用审问技巧的同时，如果能准备几张光盘，里面嵌入几个含有恶意代码的PDF，就很容易使目标中招。

一位熟人曾给我发过一份文件，标题是"采访和审问"，该文件被美国国防部用于训练其工

作人员通过测谎仪。文件列出了专业审讯者使用的不同方法，我将其列在这里。通过了解这些不同的方法，你可以学到各式各样的方法，达到社会工程的目的。

- **直截了当式**　在使用这种方法时，审讯者要装出信心满满的样子。审讯者的态度和方式彻底排除了犯罪嫌疑人无辜的可能性。在没有任何威胁的情况下，审讯者通过告诉嫌疑人"任何人都有可能这样做"来解除对方的防备。

  作为一名社会工程人员，你也可以根据伪装的不同运用这种方法。也许你伪装的是管理者、顾问或其他比目标地位高的角色。这意味着你必须有信心，并且假设目标"应该"对你的问题作出反馈。
- **间接式**　嫌疑人详细述说案发时他正在做的事，审讯者寻找遗漏、矛盾和失实的地方。审讯者的工作是让犯罪嫌疑人知道最好的方法就是说实话。

  社会工程过程中的应用可以是这样，不带任何身份色彩地接近目标，但是通过诱导或者精心设计的问题从目标那里套取信息。让目标对象成为谈话中的主角，你可能会从中得到一些信息。
- **博取同情式**　国防部手册针对这种方法提供了一些非常好的思路。审讯者压低声音、小声地说话，给人留下善于理解他人的印象。他靠近嫌疑人坐下，也许还会将手放在嫌疑人的肩膀上或拍拍他的手臂。适时的身体接触也很有效。

  社会工程人员可以像审讯者那样使用这种方式。也许你在门口等待的时候无意中听到一些员工抱怨自己的老板。也许你跟随目标去了当地的酒吧，并在谈话中表示对目标近况的同情。任何地方都可以使用这种方法，这非常有效。
- **情绪激发式**　这种方式主要作用于嫌疑人的道德或情绪层面。在审问策略方面，可以这样问："你的妻子或孩子对此会怎么想呢？"这种围绕情绪展开的想法会使他情绪低落、让他紧张，随着这些情绪的显现，审讯者便可以加以利用。

  社会工程人员可以像前面讲解的那样使用这种方式，从而抓住目标暴露出来的弱点。有一次，我得知目标偏爱参与为癌症患儿举办的慈善活动。利用这些情感，我让他做出了本不应该做的举措，并使他妥协。
- **合乎逻辑式**　这种不带情绪的做法直接呈现强有力的犯罪证据。审讯者要像商务谈判一样挺直腰杆、一脸严肃地端坐在嫌犯面前，充满信心。

  你也可以使用这种实事求是的方式为自己的出现提供合乎逻辑的有力证据，例如不论是着装还是装备都是IT维修人员的模样，同时摆出一副信心满满、本来就应该在那里的样子。
- **咄咄逼人式**　对于审讯者来说，信息收集和权利侵犯仅一步之遥，二者之间的界线不能逾越。可以提高音量，做出咄咄逼人的神情和动作，但绝对不能侵犯嫌疑人的公民权利。

  社会工程审计人员必须牢记这一界线。在第4章提到的惠普案例中，受聘对公司进行审计并没有给你触犯民法的权利。大多数情况下，聘用你的公司没有权利允许你监听家庭电话、阅读个人电子邮件或侵犯公民隐私。

- **组合式** 审讯者可以将两种方法相结合以达到最好的效果，这取决于犯罪嫌疑人的个性。社会工程人员可以使用相同的战术——组合攻击方法以期达到最好的效果。例如在发现目标的一些个人信息（比如他们最喜欢的本地酒吧）后，你可以接近目标并展开对话。这样的战术，尤其是在轻松的气氛中，对于让目标敞开心扉大有裨益。
- **处之泰然式** 这种做法非常有趣，因为审讯者的行为让嫌犯感觉案子已经结了，他认罪与否已无关紧要。这种情况下，审讯者会尝试操纵犯罪嫌疑人说出他所知道的案发经过。作为一名社会工程人员，如果不被抓到，你可能不会使用这种方法。如果在某个本不应出现的地方或场合被抓，不要惊慌失措，要让他人觉得你很淡定。你的淡定会让抓住你的人极大地降低警觉，也给予你一个消除疑虑的机会。凯文·米特尼克（更多关于米特尼克的信息可以参见第8章）非常擅长这种战术。他可以不经大脑地迅速做出反应。此外，在危险的场合表现出淡定，可以让他获取到很多信息。
- **保全面子式** 审讯者可以将罪行合理化，给嫌疑人一个机会及理由供认事实，保全他的面子。不过，审讯者不应把理由设计得太好，以至于犯罪嫌疑人在法庭上用它来为自己辩护。

  社会工程人员也可以利用这种方式。审讯者不希望给对方太好的借口，但社会工程人员可以。最好这个理由能够好到让目标不假思索就知道这只是一个为了配合你的借口。

  一种方法是说有更高级别的人叫你过来，接下去你可以这么说："我能理解你此刻的为难，但是如果在史密斯先生周一回来之前我还没有将他的邮件问题搞定，我不敢想象他会有多沮丧。"这种方式会给目标挽回面子，同时他也会满足你的请求。
- **自尊心膨胀式** 这种方式的关键是令对方感到自豪。想要它奏效，你需要找到嫌疑人的一项非常自豪的成就。吹嘘他的长相、机智或整个犯罪的精妙过程可能会使他的自尊心急剧膨胀，诱使他急切地认罪，以表明他就是那么聪明。

  在社会工程过程中，社会工程人员经常使用这种方法。通过鼓吹目标对象的成就，得到他们的最高机密。在美国核工程师的案例中（参阅第3章），在社会工程人员的夸奖和吹捧下，他说出了本不应该泄露的机密信息。
- **夸张式** 如果审讯者夸大犯罪事实，犯罪嫌疑人可能会承认案发的真实情况。举个例子，如果审讯者想把强奸罪扣到一个小偷的头上时，可以这样说："要不然你为什么会在半夜闯入他人卧室？"这种问法往往会令犯罪嫌疑人承认只是想偷窃，并非是要强奸。

  你也可以使用这种方法夸大你想要执行的任务。通过夸大去那里的理由，可以促使目标为你提供稍低的访问权限。例如，你可以说："我知道史密斯先生希望我来修理他的电脑，因为他丢失了大量的数据，但是如果你感觉不合适的话，我可以通过公司的另一台电脑来解决他电脑的问题。"
- **循序渐进式** 嫌疑人很少会立即承认自己的所有罪行。试着让他逐步承认，例如他当时在现场、拥有涉案的武器或拥有类似的车，随着事实的积累最终形成完整的供词。

  也许在社会工程过程中你会被拦在门口，门卫不让你进入大楼。这时你可以试试是否可以通过以下台词找到突破："我明白史密斯先生很忙，不能与我见面。你介意把我们的产品

信息光盘交给他吗？我将在今天或者明天给他打电话。”

这是一个较小的切入点，但如果你自己不能进入的话，那么至少要将你的工具送进门。

#### 6. 最终目标

作为一名社会工程人员，如果想要使用合适的采访或审问战术，你可能得自己先回答几个问题。我建议你将问题写在记事本上，因为这样能够帮助你在面对目标时已有充分的准备。此外，将答案写下来并进行实战演练，会给你的审讯准备工作提供思路。

请回答下面这些问题。

- **人物**　要审问或面对的人是谁？他扮演什么样的角色？列出姓名、职务以及其他有关审问的信息。
- **事件**　已经做了哪些询问准备工作？审问的目标是什么？必须有一个明确的目标。
- **时间**　询问安排在什么时间段？白天或晚上的什么时候？工作环境中的什么因素让你决定采取行动的时间？打听到什么聚会信息了吗？大部分员工此时都在休假吗？是午餐时间，还是在保安人员换班期间？
- **地点**　询问的地点在哪里？要到目标对象所在的地方吗？跟踪他去健身房、当地的酒吧或托儿所？从目标处获取所需信息的最佳场所是哪里？
- **原因**　虽然人们经常听到孩子们问为什么，但这里还是必须得问。询问的目的是什么？要目标说出某样东西的下落？让他泄露一些不该泄露的信息？为了进入一个房间或访问某个服务器？
- **方式**　审问时使用什么方法？NLP？嵌入式指令？人性缓冲区溢出（在本章结尾讨论）？还是微表情？

当然，刑事审问的目的是让嫌犯供认犯罪事实。对于社会工程人员来说，“审问”目标所要得到的信息是不同的。你想让人们在舒服的状态下为你提供信息，运用前文所述的审问战术，更易于获取信息。总之，社会工程中的询问过程应该像采访一样顺畅。不过，社会工程人员在对目标进行采访或询问时，可以使用其他一些技术进行辅助。

### 5.4.2　手势

鉴于文化的不同，手势的含义可能会迥异。不像微表情那样具有普遍性，美国人常用的手势在世界其他地区可能被认为是侮辱，或没有任何意义。

这里通过一个小练习来帮助你更好地了解手势的差异。如果愿意的话，你可以用几分钟的时间写下答案。鉴于文化不同，答案会非常有趣。

写下你所理解的这些手势的含义，以及在每一场景下是否是不礼貌的表现。

(1) 将你的手掌朝上，用你的食指指向他人并召唤他过来。
(2) 用食指和中指做出一个“V”符号。
(3) 坐下来时露出脚底。
(4) 用手指做出“OK”符号。
(5) 手掌朝外挥动你的手。
(6) 上下点头。

如果你已经写下答案，与以下有趣的文化差异进行比较。

(1) 在美国这个手势仅仅意味着“到这里来”，但在中东或远东地区、葡萄牙、西班牙、拉丁美洲、日本、印度尼西亚和中国香港地区，这种召唤人的方式被认为很无礼或侮辱人。手掌朝下并弯曲所有手指来示意，会更容易让人接受。

(2) 这个手势在美国是一个“和平的象征”，但在欧洲它的意思是“胜利”。如果手掌朝脸，它意味着“没门儿”。

(3) 在美国这是一个舒适的坐姿，并无任何恶意。然而在其他国家，如泰国、日本、法国以及中东和近东地区，露脚底意味着不敬。露出你身体最底下和最肮脏的部分是一种侮辱。

(4) 在美国这个手势表示一切正常。但是在世界其他地区有很多不同的含义：在巴西和德国，这是一个猥亵的手势；在日本这意味着“钱”；在法国则意味着“没有价值”。

(5) 在美国这是一种问候，一种打招呼或表示再见的方式。在欧洲它可能意味着“不”，而在尼日利亚则是一种严重的侮辱。

(6) 在美国点头是表示认同的一种方式，类似于说“是的”。在许多地方都是同样的含义，但在某些地区，例如保加利亚和希腊，点头意味着“不”。

这些只是在不同地区或者面对不同对象时具有不同含义的几个手势的例子。明白手势的各种含义非常重要，因为沟通本身往往比谈话内容更为重要。

本节是为了表明，在和目标对象的互动过程中，不仅需要观察这些原则，还要积极地运用它们，以操纵目标进入最容易被社会工程的状态。了解将要接触的目标对象的文化背景，避免因错用手势而带来不好的结果。

#### 1. 锚定

如果使用得当，手势可以产生很大的影响。这些手势原则中的一部分来自对NLP的研究，但是当你试图将目标对象的思维置于你的控制之下时，它们可以起到很关键的作用。

方法之一便是*锚定*，就是用特定的手势与一种类似表述形成关联。例如，你在和目标说起一些正面和美好的事物时，可以重复并且仅仅是右手做出手势。如果是坏事，则可以只用左手去比划。在做这个手势几次后，你就能开始在目标的脑海里“锚定”了一个“事实”：右手动作和美好的事物相关联。

销售人员使用这种方法来进一步强化“他们的产品”或“他们的服务”是最好的，而竞争对手的却不是。一些政客使用这种方法将积极的想法或他们想要听众认为是积极的想法与特定手势进行锚定。对此，比尔·克林顿是个范例，他深谙此道。

#### 2. 镜像

还有一种被称为镜像的手势战术，指的是你尝试匹配目标的个性化手势。当然，这并不像听起来那么容易。但是仅仅通过观察目标对象能够得到什么信息？他害羞吗？他说话大声、个性外向吗？如果在接近一个胆小的人的时候，你的动作和声音都很大，肯定会把他吓跑，甚至可能直接导致你的社会工程失败。同理，如果你很内向的话，在与“大嗓门”的人打交道时则必须镜像“大嗓门”的手势。镜像不仅包括模仿目标的肢体语言，还包括模仿他的手势，让对方更容易跟着你的思路走。

你可以将这个原则运用到另一个层次。目标对象在看到熟悉的手势时，会有一种自在的感觉。不过必须要把握好分寸，因为如果目标有一个特别的手势用得比较多，而你也在同样的情况下使用，这可能会产生激怒他的风险。要模仿他，但不要完全相同。如果目标在思考结束时手总是放在下巴上，那么你可以把手放在脸的一侧或用手指轻敲几次下巴来作为呼应。

下一节进一步分析了手势这一话题，讨论目标对象双臂和手的摆放位置的重要性。

### 5.4.3　双臂和手的摆放

执法人员在培训时就强调观察采访和审问时目标手臂及手的摆放和位置。在审问期间，动作的增多或者“坐立不安”能够显示其压力越来越大，标志着审问正在产生预期的效果。当然这是在执法环境中；社会工程场景中，你会看到相同的迹象，但目标的压力迹象可能表明你需要适当后退，除非你的目的就是要通过压力吓退他。

某些执法人员被教导要注意如下几个标志。

- 当一个人处于放松状态时，肘部一般会没有拘束地放在身体两侧。当感到威胁或害怕时，身体的自然反应是肘部向胸腔收进。从本质上来讲，在受到威胁时，这一反应为内部器官提供了一层保护。
- 手势也往往会透露很多信息。目标对象可能会用手势描述出一些不会说出的东西。例如，在刑事审讯过程中，嫌犯可能使用手势来描述作案过程（即绞杀、射杀及刺伤等），但词句中只会提到犯罪或事件。观察对象可能使用的手势的微妙变化很重要。

记录目标感受到威胁或害怕的迹象，有助于你调整战术使他们重新放松。当接近目标时，在开口之前，你的肢体语言、手臂和手势可以传递出很多信息。

其他值得注意的手势包括以下几种。

- 一个张开的手掌可能表明诚意。

- 指尖搭在一起，表明这个人认为自己很权威。
- 敲击或击打手指可能表示焦虑。
- 摸脸可能是思考的迹象，触摸头发可能显示不安，触摸耳朵可能表明犹豫不决。

一方面，注意这些手势可以为你揭示目标的很多内心活动。另一方面，如果这是你的伪装的话，这些动作有助于你饰演其中的一个角色。

从社会工程的角度来看，这里列出了一些关于手势的关键点，如果你和我一样是“手势狂人”，则很有必要掌握。

- 不要刻意去记手势，而是要记住其附加的信息。如果人们经常说“哇，那家伙做的手势真多”，你就需要少做些手势了。重要的是消息，不是手势。
- 避免单调。即使是运用手势，你也可能让人感到平淡、无聊和重复，此时手势可能让目标对你产生消极的看法。
- 注意不要表现出焦虑，如敲击手指或者做出剧烈的动作。这些动作告诉目标你很紧张，会分散听者的注意力。
- 手势太多也不行，过多的手势也会令听者分心。

请记住，要综合使用面部表情、手势和姿势。它们必须融合在一起，达到一种平衡，以支持你的伪装。

与所有这些信息同等重要的是，审问过程中用到的任何一个工具都可能成就或者搞砸你的社会工程活动。

### 5.4.4 聆听：通往成功之门

或许没有任何技能像聆听那么有学问。聆听是社会工程过程中的主要部分。你必须意识到听到和聆听之间存在着巨大的区别。

一般认为，人们对于听到的东西连一半都记不住。这意味着如果你对一个人讲10分钟话，他只会记住你所说的几分钟的内容。虽然这就是人们生活中的常态，但对社会工程人员来说，这是不可接受的。

人们通常认为，决定社会工程人员取得多大成功的通常是目标所说的很细微的东西。这个领域可以极大地提高你的聆听技能，不仅仅是听到说话的内容，而且包括说话的方式、时间及所蕴含的情感。所有这些因素都可以帮助你感知述说者所传递的信息。

成为一个好的聆听者听起来很容易，但是当气氛很紧张，你的最终目的是进入服务器机房，而你在听出来抽烟的几个员工（你想跟着他们进到大楼里）的闲聊时，要做到真正的聆听是很难的。

然而这正是需要认真聆听的时候。或许苏珊开始抱怨她的上司——人力资源部经理琼斯先

生。她讲述最近他对她是多么地粗暴无礼，她已经受够了这样的日子。然后烟友贝斯说："好吧，你应该去会计部看看，那里也到处都是笨蛋。"

或许这听起来只是两个疲惫不堪且极为恼怒的员工在喋喋不休地抱怨。是否还有别的信息泄露出来了呢？你能听到她们的名字、主管的名字、所在部门的名称以及一些员工的日常举止和行为。如果之后要提供被允许进入该办公楼的证明，这些信息就大有用武之地了。

通常一个人讲话的方式可以透露很多信息，但是要将这些信息运用到实践中则需要多听。这个人是生气、沮丧还是开心？他的语速是加快了还是变慢了？他的情绪是越来越激动还是逐渐平静？关注这些方面有时可以告诉你很多弦外之音。

那么如何成为一名优秀的聆听者呢？

接下来的步骤有助于完善聆听技能。这些建议不仅在社会工程中有所帮助，在日常生活中亦是如此，当把它们应用于社会工程审计中时，过程和结局会有很大的不同。

(1) 集中注意力　高度关注目标对象。不要鼓捣你的电话或别的小东西。不要拨弄或者敲手指。在对方说话时看着对方，将注意力集中在对方所说的内容。要充满好奇地去听、去看，不能让人感觉害怕，觉得你是在"刨根问底"。

尽量不要提前思考，不要急着去策划下一步反应。如果你在计划下一步反应或者想着辩驳，就不能集中注意力了，就可能错过一些重要的东西或者给目标留下你并不是真的关心的印象。这个很难去控制，所以对大多数人来说改掉这个习惯会花费很多功夫。

同时，尽量不要被环境因素影响。背景中的噪声或者一串笑声会转移你的注意力，不要允许这样的事情发生。

最后，还要密切关注说话者的弦外之音。肢体语言、面部表情和其他一些交流时流露出的信号也要注意"聆听"。

(2) 提供你在聆听的证据　表现出真诚并且用肢体语言和面部表情来表明这一点。不时地点点头，不用太频繁，但是要足以让对方知道你在听。你当然不想成为只会机械点头的玩偶，但是你要让目标知道"你在听"。

不要忘记十分重要的微笑。微笑可以让目标对象觉得你在和他真诚地交流，并且知道他在说什么。如同之前所提到的"集中注意力"一样，要在合适的时候加入一些微笑。如果人家告诉你他的狗刚刚死去，那么点头微笑对你来说就没什么好处了。

(3) 提供有价值的反馈　个人信仰和经验的差异会过滤掉一些信息，这点再普遍不过了。如果是这样的话，你可能"听不到"对方在说什么。

确保所问的是相关的问题。如果他在讲述蓝天，而你问"到底有多蓝呢？"是不会有作用的。

你的问题必须表现出你在积极地聆听，并且有很强的欲望去获取更深入的理解。

时不时地重述或者概括你所听到的东西就很管用。不要像做读书报告那样去背诵，而是要简明地概括主要想法，这样会使目标感觉你听进去了。

(4) 不要打断对方　这一点不用多说。打断对方的讲话显得你不顾及他的感受，并且会扰乱说话者的思绪。让他完整地述说后你再发言会更好。

然而，有时候打断确实很有用，或者不失为一种策略。电影《潜行者》（*Sneakers*）中就有类似的情节。当罗伯特·雷德福（Robert Redford）试图进入一扇大门时，他与门卫就一些快递的东西发生激烈的争论。他曾经这样干过几次，最终促使看门人示弱，让他在没有得到授权的情况下进去了。如果你认为对你有益，打断对方说话也可能是个好方法。但是大多数情况下并非如此。

(5) 适当地反应　这是区分聆听技巧好坏的分水岭。如果你专注于反驳或者下一个观点，或者在想刚才经过的金发美女，那么还是赶紧闭嘴吧。

有一次培训一组人，我在跟他们详述操纵战术的一些方面。我看出有两个家伙根本没在听，于是随便讲了一句话："然后在350度的高温下，把一只狮子烤15分钟，它就脆了。"其他人哄堂大笑，然后我转向他俩其中之一说："你觉得如何呢，约翰？"他立马愣住了，并且结结巴巴地说："嗯……是的，听起来不错。"

永远不要对目标那样做。这是对融洽关系的致命打击（本章后面会对此进行详述）。务必保持尊重，注意自己的情绪，在和目标交谈的时候务必时时作出适当的反应。

集中注意力、提供证据、提供积极的反馈、小心翼翼不要去打断对方及作出适当的反应，这些都是聆听时决定成败的关键原则。它们在长时间的社会工程会面中尤其重要，比如当我不得不在某商务会议中和一位先生会面时，我将"会面"地点设定在吧台，与他谈论生意上的东西。我想要的很多信息会在看似平常的谈话中不经意地被泄露出来。一定要在家里或办公室里训练这些技巧，让它们能在这种谈话机会出现时派上用场。你需要把好的聆听技巧变为本能，而不需要绞尽脑汁地去想。

在聆听过程中，另一个必须要考虑的因素是你个人的情感。比如我是在一个非常严厉的意大利宗教家庭里长大的，从小就被教育要尊重女性，想到有一次我用一个轻蔑的方式称呼妈妈就不寒而栗。告诉你吧，我被狠狠地教训了一顿。多年后的一天，我和一位先生交谈，并且尽力想从他那里得到些信息。我在一次社交活动中接近他，并聊了起来。他开始用一种非常不当的方式谈起一个女同事。受成长环境的影响，我的内心极为愤怒。我艰难地压制着怒火，但是愤怒肯定还是体现在了我的脸上和肢体语言上，这导致了我的失败。从这次失败中，我学到了很重要的一课：在社会工程需要聆听的场景中，你必须极力压制那些内心的成见，以免影响你取得成果。

同样，要记住对信息而不是对人作出反应。如果你不赞同一个人的信仰或立场，给他足够的面子，可以使对方感觉跟你相处非常舒服。甚至在不赞同时，你可以聊聊别的来转移注意力。举例如下。

> **目标：**“这个工作糟透了。工作时间安排得很糟糕，而且工资也很少。”
> **你：**“听起来你已经受不了这里的工作了。”

虽然你想到的可能是“努力吧”，但是用这种方式可以让目标知道你在听，并且对他的困境表示同情。

这种技术叫做反射式响应。反射式响应具有几项基本原则。

- 积极聆听，如同前面所说的那样。
- 当需要作出回应时，注意自己的情绪。了解目标说话时候你自己的感觉有助于你给出适当的反应。
- 重复内容，但不能鹦鹉学舌，而是用你自己的语言。
- 可以用一些含糊的语句来作出反应，比如“听起来像”、“似乎”或“好像”。这些语句缓和了你想要传达的信息。如果需要证明的话，下次在和同事、老板、父母或者其他人发生争执时说“你因为……生我的气”，记下他们的反应，然后换种方式说“似乎你是因为……而生我的气”。对比这两种反应，你就会发现哪一种方式更好。

反射式响应与积极聆听一起使用时，是构建信任和融洽关系的致命武器。

当学着去更好地聆听并且使之成为天性的一部分时，你将提高对听到的信息进行反应的能力。社会工程的目标是收集信息，进入那些不允许你进入的地方或者获取无权得到的信息，或者促使目标做出常理下不会做的行为。心里总是想着自己必须非常擅长操纵他人，往往会阻止你学习并练习重要的聆听技巧，但这恰恰是你需要成为一个优秀的聆听者的原因。

设想以下两种情形。

- 一位邻居走过来，问你是否有大约一个小时的时间去他的车库，帮他完成一个项目。这位邻居有一只狗，曾经好几次钻进你的垃圾箱，而且喜欢把你的院子当做厕所。在经过漫长的一天后，你正要坐下来放松，看看电视或读读书。
- 一个儿时的玩伴走过来，告诉你他需要有人帮忙搬一些家具。他刚在离你家5英里的地方买了房子，但是不能把沙发搬上楼。而你此时正要坐下来休息片刻。

哪一种情况会令你更愿意放弃休息呢？大多数人会倾向于第二种情况，但会找出拒绝第一种情况的借口或理由，或者至少要推迟到另一天他们不是那么“忙”的时候。

为什么呢？人们和朋友在一起时通常会感到放得开和自由。当你感觉和某人在一起非常舒服的时候，你们之间将没有界限，并且在帮助他们的时候会撇开自己的回报和需求。人们会很自然

地相信朋友的信息，而对来自一个陌生人的信息则会再三揣摩到底是什么意思，考虑这些信息是否值得相信。这种朋友间的关系，通常被称为“共识”。

多年来，共识仅仅在我们谈到销售人员、谈判代表以及类似人员的时候才会提到。共识并非销售人员的专属。它是一种所有人都可以使用的工具，尤其是社会工程人员。如果你想知道如何快速建立共识，请继续阅读本书。

## 5.5 即刻达成共识

我以前的同事托尼经常说达成共识比呼吸还要重要。对此，我持怀疑态度，但是共识关系的建立在社交中至关重要却是真理。

维基百科是这样定义共识的：“无意识的人类互动的最重要特性或特征之一。是看法上的共性：与交谈的另一方达成‘同步’或者‘处于相同的波段’。”

为什么要在本章讨论共识呢？这是与他人建立关系的一个关键因素。如果没有共识，对话将会陷入僵局。从社会工程背后的心理学原则来讲，共识是支柱之一。

在讨论社会工程人员应如何运用共识战术之前，你必须知道如何建立共识。建立共识是社会工程人员的一个重要工具。

想象一下，如果你能让遇到的人乐于和你交谈、想要告诉你他们的人生故事，并且想要信任你。你有没有遇到过这种人，也许只是刚刚认识，但是你会很自然地将很私人的事情告诉他？对此，虽然很多心理学因素可能也起到了作用，但也许只是因为你和那个人有共识。

后面的小节将概括建立共识的要点，以及在社会工程当中如何运用共识。

### 5.5.1 真正地想要了解他人

别人对你有多重要？你喜欢结识新朋友吗？这是一种生活的心态，不是可以教会的。建立共识的前提是喜欢对方，因为人们可以看穿虚情假意。

想成为一名优秀的社会工程人员并灵活运用共识，人对你很重要。你必须喜欢别人并且乐于和他们接触。你必须想要了解别人。人们可以识破虚假的微笑和关心。建立对目标的真正兴趣可以使你更容易建立共识。

### 5.5.2 注意自身形象

对于那些影响你和别人交往的东西，你可能无法改变，正如人们可能因为你的肤色、性别或年龄拒绝和你接触。你不能控制这些因素，但可以掌控自己的仪表，例如着装、体味、个人卫生、

眼神交流、肢体动作和面部表情。我曾读到过这样一个句子："如果一个人自己都感觉不舒服，那么别人对他也不会感觉很舒服。"这句话已经被无数次证明是至理名言。

留心你的伪装和目标。如果伪装成门卫，要确保你的举止、着装、神态及措辞和该职位的人一致。如果伪装成商务经理，要确保你的言行和着装得体。这需要研究，但是如果忽视这些因素的话，它们就会成为毁掉你与目标间达成共识的最根本原因。你的目的是在某些情况下保持目标处于防备意识较低的自动认可模式，而不是去质疑你。如果衣着、素养及举止不得当的话，就不能得到目标的自动认可，因而会降低你的成功率。

### 5.5.3　善于聆听

阅读之前的章节以了解更多的细节。善于聆听的重要性再怎么强调也不为过。

不论是想交朋友，还是以社会工程为目的，聆听都是必须掌握的技巧。

### 5.5.4　留心自己对他人的影响

有一次我看见一位老太太在离开杂货店时掉了东西。我把它捡了起来，一直追她到停车场。我追上她时，她已经打开了后备箱，准备把杂货放进去。身高6英尺3英寸（约1.9米）的我出现在这个矮矮的小老太太身后，对她说："打扰一下，女士。"显然我离她太近了，让她感到不舒服。当她转过身来时，就开始尖叫："救命啊！有人打劫啊。救命啊！"

显然，我应该考虑一下在和老太太的交往中我出现的方式会对她产生什么影响。我应该意识到，老太太独自一人处于停车场时是不期望一个魁梧的男人尾随在她身后、把她吓到的。我本该从一个不同的角度走近她的。

接触目标之前，要检查自己的仪表和其他可能影响对方的个人因素。是否需要一块能够清新口气的薄荷糖？确保脸上和牙齿上没有食物残渣。尽量确保你的外表没有任何扎眼的、让别人不愿亲近的东西。

加州大学洛杉矶分校的心理学教授艾伯特·梅拉比安以"7-38-55定律"著称。该定律指出统计数据表明，人们对你的印象只有7%取决于谈话的内容，更多的是取决于肢体语言和语调。注意自己的各种表现，但同时也要注意给人的第一印象。他对你的反应可以提醒你是否遗漏了一些东西，或者你需要做些改变使沟通更有效率。

作为一名社会工程人员，要留心你是如何影响他人的。如果满脑子都是最终目的，那么你一定会给对方留下负面印象。仔细留心忖度自己的外表、措辞和肢体语言会对目标产生什么影响。你需要给对方留下开朗、受欢迎的印象。

### 5.5.5 尽量少谈论自己

我们都喜欢谈论自己，尤其是有一个很棒的故事或传闻想分享时，这是人类的天性。谈论自己无疑会破坏亲密关系。让其他人谈他自己，直到他觉得够了，这样你会被视为一个“不可思议的朋友”、“完美的丈夫”、“伟大的聆听者”、“完美的销售员”或其他任何你想得到的头衔。人们在可以谈论自己的时候会感觉很棒，我想大家都有点自恋，但是让别人去聊他自己可以使你更受欢迎。

尽量少谈论自己，这一点对于社会工程人员尤其重要。你有明确的目标，而所扮演角色的欲望会引导你作出错误判断并走上歧途。注意力没有放在目标身上是非常危险的，这将导致你和成功渐行渐远。让目标谈论他们的工作、角色和项目，你会被他们所释放的信息量所震撼。

### 5.5.6 谨记：同情心是达成共识的关键

《兰登书屋词典》是这样定义“同情”的：“对他人的感受、想法或者态度的理性认同或者感同身受的体验。”现如今，许多人都缺乏同情心，当你觉得自己能够解决别人的问题时尤甚。然而，认真倾听他人说话，尝试确定并理解其潜在的情感，然后站在他的角度去思考，可以让人觉得你是真的感同身受。

我之所以觉得有必要提及同情心的定义，是因为理解你的目的非常重要。注意你必须“理性地认同”，然后去体验那个人的“感受、想法或态度”。

这些未必总是严肃的、令人沮丧的或极端的情绪。有时甚至理解他人烦恼、劳累或不在最佳状态的原因也能对社会工程有所帮助。想象一下你开车去银行，而女职员态度恶劣，只是因为你忘了在支票上签字，她得把支票从窗口递出来。不巧你又忘记带笔，需要她再帮个忙。你的反应可能与我相似，尤其是如果她怒目圆瞪，你想要告诉她她在这里就是应该为你服务的。不过，也可以试着这样说：“你看起来似乎有点生气。我理解你的心情，当客户丢三落四的时候我也会生气。不好意思，但我还是得问你借一支笔。”

表达同情时不要显得盛气凌人，这点很重要。如果你表达同情时显得很傲慢自大，可能会让目标觉得你在以恩人自居。

你理解她的恼火却不责怪，表明了你感同身受，然后提出了请求。同情心对建立共识大有裨益，但是要注意共识是无法伪造的。人们需要感受到你是真诚地想建立信任关系。如果你不能自然地展现同情心，那么就请多加练习。与家人、朋友、同事、老师或同学练习。无论地点和方式，只要试着表达同情就能大大提高你建立良好人际关系的能力。

同情心是社会工程人员的一个工具，然而它也常常被用在恶意的社会工程中。当世界的某个地方发生灾难时，恶意的社会工程人员经常会“同情”你。很多情况下，恶意的社会工程人员之所以能够如此容易地表明同情，是因为他们本来就是来自落后、贫穷或困苦的地方。

由于自身的状况比较糟糕，让人感觉他们对于别人的困境会很有同情心，因此可以很自然地建立共识。

没有什么比让别人感觉到你“感同身受”更容易建立共识了。当一个人是某个灾难的直接受害者时，这种理论显得尤为正确。这种想法很恐怖，但那些虐待、犯罪、强奸、自然灾害、战争或其他暴行的受害者往往会“理解”那些正在经历这种困苦的人的感受。如果这种共识建立起来的话，受害者会信任错误的人。

如前文所述，当纽约遭遇“9·11恐怖袭击事件”后，许多人声称他们在恐怖袭击中失去了亲人或朋友。这引发了他人的同情，这些“受害者”也因此得到了金钱、名望或者追求的其他东西。

作为一名社会工程审计人员，你得掌握多种情感的表达。如果你的情感处于封闭状态，表达同情将变得非常困难。如果你乐于与他人交往的话，表达同情就变得非常容易。如果这么做了，你便很容易理解他们，知悉他们的故事，并对他们表达出同情。

### 5.5.7　扩大知识领域

知识就是力量。你不需要样样精通，但对各个行业都做一些了解会比较有益。这样对方会觉得你很有趣，给你制造一些谈资。

知识就是力量。这句古老黑客准则对社会工程人员依然适用。社会工程人员应该保持阅读和学习的习惯。如果你用知识充实自己的大脑，那么和目标接触的时候，就知道聊什么了。不要忽视了阅读、研究及调查目标人物的职业或爱好。你的目的不是成为“万事通”，或成为所有话题的专家，而是要有足够的知识，这样当目标问“身上有没有RJ-45接头来修复服务器的网络连接问题？”的时候，你就不至于呆呆地盯着他看。

### 5.5.8　挖掘你的好奇心

人们在对某些事情抱有思维定势时往往会变得有些自以为是。自以为是或者武断的态度可以改变一个人对所述事情的反应。即使什么都不说，你也会在心里想，这会体现在你的肢体语言或面部表情上。我们应该培养自己对别人思考及做事方式的好奇心，而不要固步自封。好奇心可以防止你作出草率的决定。在寻求帮助或请求得到更多的信息时，这会让人觉得你很谦逊。要保持心胸开阔，探究并接受别人在某一话题上的想法，即使这些想法与你的想法有所不同。

好奇心不会害死社会工程人员，对于其他人来说亦如此。当对别人的生活方式、文化和语言感到好奇时，你会渐渐明白他们的生活方式。好奇心也会让你不再陈腐或固执己见。你可能不同意某些话题、信仰或行动，但如果能保持好奇、不武断，就可以在试图理解为什么他会那样或那样做基础上接近一个人，而不是通过判断一个人来接近他。

### 5.5.9 设法满足他人的需求

此观点是这些原则的重中之重，也是本书最有力的观点之一。威廉·格拉瑟（William Glasser）博士在其著作*Choice Theory: A New Psychology of Personal Freedom*中指出了如下4种人类的基本心理需求。

- 归属/联系/爱
- 权力/地位/能力
- 自由/责任
- 娱乐/学习

这一观点背后的原理在于通过谈话使对方找到实现自己需求的方式，从而即刻达成共识。如果能够创造一个环境来满足对方的需求，你便可以创建牢不可破的关系。

让我们通过一个小故事来表明满足别人需求的作用。我曾经发生过一次不怎么严重的车祸。一位年轻的司机突然超车到我前面然后急刹车。那一瞬间，我要决定是以55英里（约88千米）每小时的速度撞上他，还是避开他然后自己撞到小山一侧的水沟里。为了保住车里3位年轻人的生命，我很快选择了后者。紧接着，车飞了出去，撞到坚硬的岩石上才停了下来。我眼看着自己定制的心爱的捷达车在巨大的冲击力下撞瘪了，我的脸也贴到了挡风玻璃上。我的车还几乎刮到另一辆车的后保险杠，但幸好我的车速很快，他的车只是停在了高速公路边上。恢复意识后，我们打电话叫来了警察和救护车。

这个年轻人和我投保的不是同一家保险公司。第二天一早，他的代理人便打来了电话，很礼貌地询问了几个问题。他告诉我保险理算员会来界定我那辆捷达的损坏程度，48小时内我收到了一张支票和一封信，信中表明他们会支付我所有的医疗费用。

几日后，他的保险代理人又打来了电话，询问我的身体状况。你觉得我的保险公司打过几通电话呢？就一通，只是告诉我该如何回答问题。

我知道关心所有客户并不是这些大公司给他们设定的岗位职责。但他的保险代理人给我打电话只是为了确认我是否已康复。我顺利得到了理赔，对车的赔偿也很合理。

两天后，我取消了和原保险公司的合约，去见了埃里克，也就是那个导致我撞车的年轻人投保的保险公司的代理人，他曾多次给我打过电话。我告诉他，他给我留下了深刻的印象，我想要买他出售的保险产品。从那时起到现在已经12年了，我的所有保险都是埃里克代理的。大约两年前，我接到了一个保险公司的电话，给我提供的保险价格比埃里克公司的低很多，但我完全没有考虑换代理人。为什么呢？共识——清楚而又简单的道理。埃里克是我的朋友，也是我的帮手，我可以打电话向他咨询保险问题，而他总是会给出最佳方案。他关心并且了解我的家庭，而且从不强行向我兜售保险。不过他也完全没必要这么做，因为只要是他代理的保险我都会买，我信任他。

这就是共识的力量。也许埃里克所做的一切只是为了让我买他的保险，对于这一点我不是很清楚，但持怀疑态度。我了解他，他是发自内心地关心，而且认识他的人也都这样认为。他和兄弟的生意做得很好。可见，共识可以在人与人之间创建超越得失的关系。

满足对方的需求可以大大增加建立共识的机会。不要让对方觉得你别有用心，而是真心诚意地去帮助他，结果会让你大吃一惊。对于社会工程人员来说，也许没有别的方法比满足对方的需求更有价值。学习如何创造一个使目标感到舒适并满足其4种基本心理需求中一种的环境，是建立牢不可破的共识的可靠方法。

间谍经常使用这个原则来满足别人的需求或期望。在最近去南美洲国家的旅行中，有人对我说，他们的政府一直通过满足最基本的“联系/爱”的需求完成渗透。他们会送美女去勾搭男人，但这不是一夜情。她会一连几天、几周、几个月甚至几年来引诱他。随着时间的流逝，她会更加大胆地要求去对方最私密的地方，最终会到他的办公室，在那里她会获得访问权限去植入漏洞、木马或者复制硬盘。虽然这种方法会产生毁灭性的效果，但是非常管用。

社会工程人员也会通过钓鱼电子邮件来满足欲望。在一次测试中，我们向一家知名公司的125名员工发送了邮件，邮件中含有名为“布兰妮裸照”、“麦莉・赛勒斯入浴图”等虚假图片文件，其中每张图片都含有恶意代码，社会工程人员可以通过它们访问用户的电脑。结果表明75%以上的图像都被点击了。而且我们发现明星越年轻，点击率越高。

这些令人恶心和具有灾难性后果的事实表明，满足人类的欲望可以起到很大的作用。对个人来说亦是如此。警方的审讯人员一直使用这种战术来建立共识。

有一次，我在“social-engineer.org”播客节目（详见www.social-engineer.org/episode-001-interrogation-and-interview-tactics）中采访了一名执法人员。他讲述的故事证实了共识在让人们服从要求方面的巨大作用。警察逮捕了一名偷窥狂。他有一种癖好，就是爱侵犯穿着粉红色牛仔靴的女人的隐私。执法人员并没有一味指责他的变态行为，而是这样说的：“我也喜欢红色的……我前几天也看到这个女孩穿着热裤和长筒牛仔靴，哇哦!”

他很快就放松了。为什么呢？因为他觉得自己与志趣相投的人在一起，认为他与大家建立了联系，融入“集体”之中了。那些评论让他很放松，于是开始讲述自己的“爱好”。

虽然在如何开发和建立共识方面，这是一个范例，但是作为社会工程人员，该怎么使用它呢？

通过运用前面讨论的原则，你可以在数秒钟内建立共识。为了证明这一点，设想一下，你需要提取一些现金，身上没带银行卡，而且记不清银行卡账号，所以你必须向银行职员寻求帮助。询问自己的账号也许会有点尴尬。你走进银行卡开户行的本地一家支行，不过之前你从未来过这家支行。银行里没有拿号排队的人，你可以自己选择柜员。或许你不会考虑这些，大多数人都不会考虑，不过你会观察所有对外开放的窗口，并选择一个自己感觉最舒服的柜员。虽然在所有窗口都将得到同样的礼遇，但是你会选择那个让你觉得舒服的窗口。

也许你会选择最有魅力的人，或者一个带着最灿烂笑容的人，或者第一个问候你的人。无论你选择谁以及怎样进行选择，不管是有意的还是无意的，绝大部分选择都会与共识有关。对你和目标来说，这一原则同样奏效。当走向目标对象时，他将依据你的外貌、风度、面部表情，当然，还有他的心情形成对你的第一印象和判断。其中的大部分因素都是可控的，所以应该预先准备来提高成功率。

适当地建立共识能创造强力胶一般的亲密关系，能承受小的不便，甚至是一些误会。

共识让人们说和做只有好友之间才会说和做的事情，因为你已经信任他了。这是一股强大的力量，如果没有它，销售、友谊、雇佣关系和许多其他情况将更难维系。

还记得第4章中关于伪装的内容吗？因为伪装不仅仅是表演一个角色，对目标来说你就是一个活生生的人，所以你要成为那个要伪装的角色。恰当的伪装对于建立正确的共识非常必要。在许多社会工程场合，由于没有时间虚构故事情节并使用长期诱导或共识技术，因此你的成功将建立在许多需要构建的非语言表达方面。

### 5.5.10 使用其他建立共识的技巧

其他建立共识的方法都是建立在NLP研究的基础上的。正如大家所了解的，共识基本上就是和他人建立联系并让对方感到很自在。接下来我们会讨论催眠者和NLP实践者经常用到的、可以使对方即刻放松下来的NLP技术。

#### 1. 呼吸频率保持一致

与他人呼吸频率一致并不是意味着你要密切注意目标对象的呼吸并和他的每次呼吸都保持一致。不过，有些人的呼吸方式很容易辨别，比如有些人的呼吸快而短，有些则长而深。留心目标的呼吸方式并进行模仿，但是不要盲目重复，也就是说，不需要每次呼吸都和对方保持同步。

#### 2. 语音、语调保持一致

我出生在纽约，在一个意大利家庭里长大。我语速快，嗓门大，并且会手舞足蹈。我有75%的意大利血统，还有25%的匈牙利血统。我长得又高又壮，大嗓门，并且手势做得飞快，就像一个专业手语翻译那样。在和胆小、害羞、说话慢条斯理的南方人说话时，如果我不能放慢语速、把手放好并改变沟通方式，则不可能达成共识。留心目标人物的语音特点，无论是快、慢、大声、温和抑或悦耳，试着使用与之相同的方式。但是对于口音，原则是不要模仿。除非你能运用得得心应手，否则不要尝试，不伦不类的口音会毁掉共识。

除此之外，你也可以留心听*关键短语*。有些人习惯用一些口头语，如“好的”或“是的”。不要遗漏任何关键短语，可能当时不一定用得上，但可以将其转化到随后的句子里。

我曾经遇到过一个目标对象，他喜欢这样表达数字：“这种要6个，那种要半打。”我不常用

这样的语句，而且不想勉强这样说，因为那将导致缺乏共识。不过，我从中抽出一些关键词，然后像这样说："那件事我肯定做过6次。"

他人讲话的方式也可能影响你的个人判断。有些人喜欢耳语，有些人则喜欢低语，还有些人喜欢触摸到对方。如果你的方式不同，就得让对方以自己觉得舒服的方式讲话，然后再模仿他。

3. 肢体语言保持一致

保持肢体语言一致之所以是一种非常有趣的建立共识的方式，主要是因为它能构建非常强的关系，但同样也可能在几秒钟内因为不匹配而毁掉全部共识。

如果你注意到某人以双臂交叉的方式站立，不要以为他是在排斥你，或许他只是冷了。你能将一只手臂抱在胸前模仿他的姿态，或者将双臂交叉吗？

当坐在一个正在吃饭的人对面时，你可以在他吃东西的时候呷几口饮料模仿他。不要跟他做一样的动作，但是可以做类似的动作。

人们喜欢那些跟自己相像的人，这是天性，会让他们感到舒服。比尔・菲利普斯（Bill Philips）是"Body-for-Life"程序背后的天才，改变了健身程序的开发方式。他宣扬的一些概念与镜像原则关系密切。如果你很胖而且只和肥胖的人在一起，那么就别指望会变得苗条。为什么呢？答案就在于你安于肥胖的状态，周围的人亦是如此。如果想改变，就要跟那些窈窕淑女在一起，这样心理上很快就会发生变化。

这一原则同样适用于社会工程。由于不能指望目标改变，所以你需要和他们类似，使之感觉和你在一起很棒。

### 5.5.11　测试"共识"

运用这些建立共识的技术，配合相应的积极态度及面部表情等，就可以在潜意识层面建立稳固的共识。

在尝试这些策略之后，你可以通过一些动作来测试你们的共识，比如抓抓头或摸摸耳朵。如果在接下来的一两分钟内目标做出了相似的动作，你们可能已经建立了稳固的共识。

当发展、建立和开启与他人的关系时，这些技术可以在你生活中的很多方面创造奇迹。学会运用本章中的心理学原则，会给你的社会工程实践带来巨变。

多年来人们一直认为人类的思维可以像程序一样被改写。这只是传说吗？人类的思维可以被掌控吗？

下一节将揭示本书中最令人兴奋的一些内容。

## 5.6 人类思维缓冲区溢出

杯子的容积是有限的，将10盎司的液体往8盎司的杯子里倒，会发生什么？当然是液体溢出，流得到处都是。如果强行向容器中倒入超过其容积的液体，只会使杯子在压力作用下破碎。

同样的原理也适用于计算机程序。设想一个小程序，它只有一个功能和两个字段：用户名和密码。

当程序运行时，会有一个小窗口，你在用户名字段处输入“admin”，在密码字段处输入“password”，然后一个小的消息框会弹出提示“OK”，表示一切正常。

开发人员为用户名字段分配了一定数量的内存空间，足以保存几个“admin”的字符串长度。如果你在该字段中输入20个“A”然后点击确认键，会怎么样呢？

程序会崩溃并弹出错误提示窗口。为什么呢？因为输入的字符比分配的内存空间长，并且没有正确的错误处理程序来抛出异常，所以程序崩溃了。

软件黑客的目的就是找到能够引起程序崩溃的地址，并在该地址插入恶意代码。通过控制执行过程，黑客可以让程序“执行”他想要的任何程序。他能够在程序的内存空间中注入任何类型的命令，因为他有完全的掌控权。作为渗透测试人员，没有什么比让程序按照其意愿执行更令人兴奋的事情了。

人类的思维也可以被看做一系列运行的“软件”。随着时间的累积，渐渐地你会形成自己特有的“软件包”，建立自己的指令集、缓冲区和内存长度。

在将这些应用到人类思维之前，有必要讲解下几个技术术语。缓冲区是一个空间区域，其中可以发生一些事或用来存储数据。在前面“登录程序”的示例中，密码字段有一个缓冲区，大小就是允许存放的字符数。如果输入的字符数比缓冲区大，程序员就应该告诉程序如何处理更大的数据集。

如果没有做处理，计算机就会崩溃，程序也就关闭了。通常，后台的情况是这样的：程序不知道该如何处理所有的数据，从而溢出了分配的内存空间，程序直接崩溃并退出。此谓缓冲区溢出。

人类思维的运行模式亦如此。我们为特定数据集分配了空间，如果特定的数据集不能放入申请的空间，会发生什么呢？不像计算机，大脑不会崩溃，但是会出现短暂的空档期，这个时候就可以植入命令，通过额外的数据告诉大脑该如何做。

人类思维缓冲区溢出基本上也是同样的道理。我们的目的是识别出运行的“程序”，并向程序插入代码，使你能够植入命令，从根本上控制思维导向。

可以通过一个很简单的例子测试这个概念（如图5-16所示）。

因为本书是单色印刷的，所以我将彩色版本放到了www.social-engineer.org/resources/book/HumanBufferOverflow1.jpg上。

测试要点是这样，打开前面的网址，尽量快速地说出图片中单词的颜色，而不是读单词。

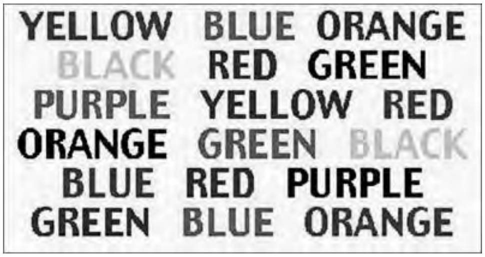



图5-16　人类思维缓冲区溢出实验一

这个游戏并非表面上那么简单。如果你成功通关，可以试试不断加快朗读速度。对于大多数人（如果不是所有人）来说，至少有一次你会习惯性地读出单词，而不是其颜色，或者你会发现自己在整个过程中都很挣扎。

为什么这个实验这么难呢？因为植入的命令。我们下意识地要读出这些单词而不是其颜色。这就是人类大脑连接的方式。大脑看到了颜色，但是首先会对单词的拼写作出反应。也就是说，思维中出现的是单词而不是其颜色。这个实验显示人类大脑中执行的代码可能会与人们想到或看到的相反。

## 5.6.1　设定最基本的原则

在一篇名为Modification of Audible and Visual Speech的论文（详见www.prometheus-inc.com/asi/multimedia1998/papers/covell.pdf）中，米歇尔·科维尔（Michele Covell）、马尔克姆·斯兰尼（Malcolm Slaney）、克里斯托弗·贝格勒（Cristoph Bregler）和玛格丽特·威斯考特（Margaret Withgott）4位研究员共同指出，科学家已证明人们在一分钟时间里只能说出150个单词，但在同样的时间里却能够思考500~600个单词。这就意味着大多数人在听你说话时大脑会快速思考。所以想通过提升语速来使听者脑部缓冲区溢出几乎是不可能的。

你还得明白人们在日常生活中是如何作决定的。人们所作出的大部分决定都是下意识的，如怎样开车上班、冲咖啡、刷牙及穿什么衣服等都没有经过真正的思考。

你有没有过这样的经历呢？开车上班，到了公司之后，却不记得经过了哪些广告牌、走的哪条路或者新闻中播报了什么交通事故。你处于下意识掌控的思维状态，不需要有意识地去考虑每个转弯，只要按照惯性开就可以了。

人们的大多数决定都是这样作出来的。有些科学家甚至相信在正式作出决定7秒之前，潜意识就已作出了决定，其后才在现实中反应出来。当人们最终有意识地作出决定时，他们的决定不仅依据听到的内容，决策过程还会涉及视觉、感觉和情感。

弄清楚人类工作及思考的方式是创建缓冲区溢出的最快方法，或者说是创建人类思维固有程序溢出的最快方法，弄清楚之后，你就可以植入命令了。

## 5.6.2 人性操作系统的模糊测试

在实际的软件攻击中，模糊测试（fuzzing）方法能够用来寻找可以重写的软件错误，使得恶意黑客获得实际的控制权。模糊测试中，黑客向程序发送不同长度的随机数据，以测试因不能处理数据导致程序崩溃的情况。这样黑客就有机可乘，从而嵌入恶意代码。

和程序的模糊测试一样，你必须明白人类思维对特定类型的数据是如何反应的。通过观察人们在面对不同决定和数据时的反应，就能够知道他们运行的“程序”如何。人类思维中的有些行为准则似乎是与生俱来的，每个人都会遵守。

例如，一栋大厦有内外两道门，你为一个陌生人开了第一道门，你猜接下来他会怎么做？他要么帮你打开接下来那扇门，要么等你进去才关第一道门。

在交通汇流处，你让一个完全不认识的人并到你前面，当你稍后想并道时，他也会不假思索地让你。为什么呢？

这里面的原因和预期定律有关，即人们通常会遵循一个预期。人们常常遵循他们感受到的别人的期望或要求来作决定。利用这个定律，你可以将恶意“数据”植入到对方的脑部程序，我们称之为预设。

先给目标一点甜头尝尝，接下来再提请求时就不大可能吃闭门羹。拿前文“开门”的简单例子来说，如果你给别人开了门，他极有可能至少会试图为你打开下一扇门。在提出要求之前，社会工程人员可以预先恭维目标或者提供一些他们认为有价值的信息。通过先给予，接下来有所请求就显得理所应当了。

下面的示例完美地诠释了“预设”。

“你认识我的邻居拉尔夫吗？他总是开着那辆绿色的福特雅仕。”

在这句话中，你预设了如下信息：

- 我认识这位邻居；
- 他叫拉尔夫；
- 他有驾照；

- 他开一辆绿色的车。

想要高效地运用预设方法，你要综合运用措辞、肢体语言和面部表情来问问题，从而让人觉得你所表述的是事实。这种方法最基本的一点便是穿透“防火墙”（理性状态），直入“系统最低层”（下意识状态）。最快的方式便是通过嵌入式指令注入你的“代码”，接下来会有进一步的阐述。

### 5.6.3　嵌入式指令的规则

一些行之有效的嵌入式指令基本原则如下。

- 指令要短，3~4个字即可；
- 些许强调会更加有效；
- 蕴含在普通的语句中最有效；
- 配以适当的面部表情和肢体语言。

市场营销中对嵌入式指令的运用很流行。

- “秒杀！”
- “限时特卖！”
- “即刻关注！”

在真正的缓冲区溢出中，程序编写人员会使用填充字符技术，即通过填充一些字符的方式，在不影响程序正常运行的情况下，让恶意代码得以“进场”执行。社会工程人员也会在表述时加上类似填充的语句，让后面植入的命令不至于显得太突兀。举例如下。

- “当你……”
- “当你……时的感觉是怎样的？”
- “有个人能够……”
- “既然你……”

以上这些表述均能创建一种情绪或思维，允许你在潜意识中植入代码。

关于嵌入式指令的例子有很多，这里仅列出几个供参考。

- **巧用引用或故事**　大脑在处理故事与处理其他信息方面有着很大的差异。纵观历史长河中的名师巨匠，像亚里士多德、柏拉图、迦玛列及耶稣，他们都是用故事和实例来向听众传授知识的。为什么呢？
  秘密就在于潜意识的思维将故事作为直接指令来处理。NLP的创始人之一班德勒曾告诫NLP实践人员要学会引用。他深知演讲者以故事和引用的方式去传达信息会更为有效。多读、多用引用，然后将指令嵌入其中，是对该技术的一种极致应用。

例如有一次，我需要让目标给我旧密码，以便将其“修改”成更加安全的密码。我伪装成技术支持人员，当然他们会询问为何需要修改密码。于是我采用了这样的方法：“Xavier研究公司近期的一项研究指出，在美国企业中74%的人使用较弱的密码。这就是我们推出这项强制要求在企业范围内更改密码计划的缘由。我会帮你更改密码，你把旧的Windows密码告诉我，我即刻就能改好。”通过引用研究机构的说辞，我的话变得更有分量。

- **善用否定** 善用否定利用的是人们的逆反心理。当阻止目标过多关注一件事时，往往也能在其中嵌入指令。比如说，在告诉你“不要花太多时间练习使用嵌入式命令”时，我就嵌入了“练习使用嵌入式命令”这一指令。我会预设你将进行一定程度的练习，如果你比较固执的话，可能会说：“不要告诉我该做什么，我会按照自己的意愿练习。”

  如果你告诉某人一件事不重要或不相关时，他会下意识地格外关注，这样他就能够确定这到底是否相关。就像前文的例子，有时采取否定的方式嵌入命令可以令目标别无他选，只能执行。

- **使听众想象** 当你问听众“……会怎么做”、“当……时，你有何感想”这样的问题时，该方法就会奏效，因为对方必须经过联想才能作答。如果我问“当名利双收时，你会怎么做？”，要回答这个问题，听者自然会想象自己又有钱、又有权的状态。同理，如果问“当你熟练掌握嵌入式指令时，会怎么样？”，我是在迫使你想象变成专家时会有何感觉。这样说吧，假使我告诉你“不要去想红色的奶牛”，你得先在脑海中勾勒出一头红色奶牛的模样，然后再告诉自己不要去想它。你潜意识的思维会先把指令中的每个词语构想出来，再进行下一步的指令执行。

  在读懂这个句子时，你在潜意识里已经勾勒出了句中描绘的情形。潜意识会直接处理该句子，而不会去管上下文到底在说些什么。另一个重要的方面就在于潜意识能够操控肢体语言、面部表情、语音语调还有手势，并将其与所表达的信息联系起来。也就是说，潜意识里的行为一旦被破译，加上嵌入式指令，你能做的只有服从。

值得一提的是，在嵌入指令时，语气一定要正常。如果过分强调某个单词，只会让目标觉得有古怪，从而吓坏他，嵌入指令这一目的也就归于失败了。就像软件缓冲区溢出一样，传达的信息必须与想要溢出的指令相匹配。

## 5.7 小结

也许你已经意识到了，嵌入指令的应用领域很广泛，也具有很大的出错空间。必须要勤加练习才能成功使用。不过我不推荐利用本章的内容进行引诱等行为，现实中还是能够找到一些关于引诱的得体的视频，其中体现了嵌入式指令是如何运作的。

使用这些原则能够创造一种环境，让目标对象更容易接受你的建议。

仅仅告诉目标“你会买我的商品”并不代表他会一直买。那么为什么要使用这些指令呢？

嵌入式指令创建了一个平台，使社会工程活动变得更简单。通过这些类型的指令也可以让合作的公司有所收获，教育他们目标何在，而且如果有人想尝试这种社会工程方式，就可以及时识破。

如果你想要将嵌入式指令的原则写成一个方程式，大致会是这样：

人类思维缓冲区溢出=预期定律+思维铺垫+嵌入式代码

首先，在与对象开始交谈时结合使用短语、肢体语言和假定性的言辞。假设你所要求的事情已经十全十美地完成了。

然后，通过一些语句在对方的思维中做铺垫，方便后续的植入指令操作。本质上这就是思维缓冲区溢出方程的体现。使用方程时要保守，在尝试前要进行大量的练习。在日常生活、工作中就要进行尝试。寻找一个通常不会响应简单要求的同事作为目标，尝试看他是否会为你煮咖啡。你问："汤姆，你要去茶水间呀？能帮我带杯加两份奶精的咖啡过来吗？"

不断提升指令的完成难度，看看你到底能够得到什么。尝试运用上文提到的方程从他人处获取承诺，看到底能够得到多少信息，注入多少指令。

本章涉及了本书中一些最深奥、最令人惊异的社会工程心理学原理。这一章就能改变你的生活，并且能够提升你的社会工程能力。理解人们的思维方式、思维定势形成的原因以及怎样改变他们的想法，这是成为一名社会工程人员的必修课。接下来的章节将介绍如何对目标施加影响。

# 第 6 章
# 影响：说服的力量

晓之以理，不如示之以利
——本杰明·富兰克林

富兰克林的这句格言可以说是对本章全部内容的概括和总结。读者可能会奇怪，为什么我没有将这部分内容放在第5章，作为社会工程心理学的一部分来讨论。心理学是一门科学，其中蕴含一整套规则，按照规则运行会产生一个结果。社会工程心理学是科学的，也是预先策划好的。

影响和说服更像是以科学为支撑的艺术，其中包括了情感和信仰因素。正如前几章讨论的那样，必须得了解人们的思维方式及真实想法。

影响和说服的艺术就是让他人*想要*以你所期许的方式去行动、反应、思考或建立信仰的过程。

如有必要，请再读一遍上面的句子，它可能是全书中最具影响力的句子之一。也就是说，通过使用这里讨论的原则，能够让他人按照你期许的方式去思考、行动，甚至对此毫不怀疑，而且自愿这样做。社会工程人员每天都在应用说服的艺术，不过恶意的社会工程人员和骗子也在这么做。

一些人投入了毕生的精力去调查、钻研并不断完善影响他人的艺术。例如埃伦·兰格博士（Dr. Ellen Langer）、罗伯特·恰尔迪尼（Robert Cialdini）和凯文·霍根（Kevin Hogan），他们为该领域贡献了大量的知识。将其与NLP方面的专家学者（如班德勒、葛瑞德以及近期的杰米·斯马特）所做的研究和教学工作结合起来，你就有潜质成为影响他人方面真正的艺术家。

真正的影响是精妙而顺畅的，大部分时候被影响的人会毫无察觉。掌握其中的技巧之后，你会注意到它们在商业、宣传以及销售工作中的应用，从而开始对市场人员拙劣的尝试感到恼怒。

如果你跟我是同道中人，还会在开车的时候不断抱怨那些糟糕的商业和宣传行为（对于这一点，我的妻子颇有微词）。

在正式介绍社会工程人员如何运用说服和影响策略之前，先简短介绍一下我收集和使用过的关键要素，包括回报、操纵以及设置目标的作用等。

影响和说服可以分解成5个重要方面，后续各小节将一一介绍。

## 6.1　影响和说服的 5 项基本原则

要想成功影响目标，下述说服的5项基本原则尤为重要：

- 目标明确；
- 构建共识；
- 洞悉环境；
- 灵活应变；
- 内省。

社会工程的全部目的就是影响目标采取一项不一定符合他们最佳利益的行动。他们不仅会采取行动，而且*想要*采取行动，甚至在最后还会感谢你。这种影响的力量很强大，也使得具有这种能力的社会工程人员成为传奇人物。

世界知名的NLP培训专家杰米·斯马特曾经说过："地图非疆域。"我喜欢这句话，因为它很适合用来形容这5项基本原则的关系。没有一项原则能够涵盖全部精髓，但每一个都能在地图上为你指明疆域拓展的一个方向。下一小节会详细讲述第一项原则：制定明确的目标为何非常关键。

### 6.1.1　心中有明确的目标

我们不仅要在心中有明确的目标，甚至需要更进一步，将目标写下来。首先需要问自己："通过这次活动或者交流我想要得到什么？"

我们在第5章（尤其是有关NLP的部分中）曾讨论过，人的内部系统运作受其思维和目的的影响。如果专注于某项事物，则更可能实现或者得到它。这并不是说如果你一直想着得到一百万美元，就会得到它。事实上，这是不可能的。相反，如果你的目标是赚一百万美元，并且专注于赚钱的具体步骤，那么你的目的、知识和行动会提高你达成目标的可能性。"说服"也是同样道理。你的目的是什么？是改变某人的信仰，还是要他采取某种行动？假设你的好朋友正在做的事情对其健康非常有害，你想要说服他别再那么做了，此时你的目标是什么？也许最终目标是说服他停止伤害自己，但是过程中存在很多小的目标，将所有这些目标列出来，可以使影响他的过程更加清晰。

在设定目标之后，必须问自己："我怎么知道目标已经实现了？"我曾经听过杰米·斯马特的培训课录音，他是NLP领域的世界级专家。他给教室中的所有学员提出了这样两个问题。

- 你想要什么？
- 如何知道目标已实现？

在听到第一个问题时，我将CD暂停，大声说出了自己想从这堂课中汲取的知识，随后继续听录音。在听到第二个问题时，我再次暂停CD，感觉很茫然。很显然，我并没有一个清晰的思路。虽然我知道自己想要从这门课程中学到什么，但是并不清楚在实现目标后如何来度量。

了解自己想要从事件中得到什么是影响和说服战术的一个重要方面。在明确目标并了解成功标志的情况下接近目标，就能清晰地制定出采取行动的方式。清晰定义的目标对社会工程人员所采用的影响战术的成败具有决定性意义，也使得下一步的行动更容易掌控。

### 6.1.2 共识、共识、共识

5.5节详细阐释了共识的构建。请仔细阅读和分析，完善构建共识的技巧。

达成共识的意思是吸引目标及其潜意识的注意，在他的潜意识中构建信任。掌握这一能力能够改变你和他人相处的方式。对于社会工程人员来说，这会改变你的整个思维模式。

要构建共识，首先需要从目标的心理状态入手，即尝试了解他们的心情。他们起了疑心？烦躁、悲观、焦虑？无论他们处于什么样的精神状态，只要你感知到了，就从那里入手。要将注意力集中在目的上，更要致力于理解对方，这是至关重要的一点。这就要求社会工程人员必须充分了解目标，可以想象他们的精神状态，即目标的想法和心情。

例如，你想影响一位好朋友，让他戒烟或者戒毒什么的。请注意你的目的不是说服他戒，而是让他*想要*去戒。你的目的不是关于你，对吧？也就是说必须将注意力集中在目标身上。你不能说他的这一癖好对你有怎样的影响，你多么厌恶那个味道等，重点必须放在对他有怎样的影响。你不能在言语上攻击他和他的习惯，而是必须理解和接受对方的心情，这样才能与他建立共识，最终产生影响。

社会工程中的处理方式大体上和这个是一样的：你不能完全按照自己的思路走。很多人对此会比较纠结。你知道他吸烟的原因吗？你了解他养成这一习惯的心理、生理和精神上的原因吗？只有能够真正站在对方的角度考虑问题时，才能构建坚实的共识，否则你意图影响他人的努力将归于失败。

此外，你不要总想着通过逻辑来创建共识。有一次我到医院看一位挚友（死于喉癌）。他吸烟40多年，有一天发现自己得了癌症。癌细胞扩散得很快，他只能住进医院度过生命的最后时光。

他的儿女到医院看他，但是每隔一阵就要离开病房。我想他们一定很痛苦。有一次在他们离开病房后，我跟出去想安慰他们，竟然发现他们在医院外抽烟，我顿时哑口无言。我没有抽烟的习惯，以后也不打算抽烟，虽然知道烟瘾是很难克制的，但是我不能理解，在看到父亲的痛苦后他们是怎样点燃那根烟的。

在这里运用逻辑丝毫没有用处。用吸烟的坏处和对健康的危害来劝说朋友的孩子不会奏效，因为这些话没有任何价值，只会让心情沉重的他们反感，让我一吐为快而已。在了解对方之前，你是很难通过构建共识影响对方的。

要使他人想要做一件事，需要从感情和逻辑两方面入手，很多时候还需要理解和谦逊。有一次我去某个办公室处理一些事，因为在外面听到一些有趣的笑话，所以在走进大厅的时候我一直在笑。站在接待台后的女士刚刚肯定是做了一件尴尬的事情，因为她看见我笑的时候，立刻变得很愤怒，并且大声对我说："没什么好笑的吧，你这个混蛋！"

我不认识这位女士，并且知道这件事对我心中的目标没有一丝好处。而且对于她觉得我在嘲笑她且会进行反击这件事，我觉得受到了侮辱。不过，我看到她很难受，于是走近接待台，我不是要让她更难受，而是望着她的眼睛，亲切地说："如果你认为我在笑话你的话，我很抱歉。我之所以笑，是因为在停车场的时候，你同事在说有关周末聚会的事，我认为很有趣。"

她看着我，我能感觉出她此时更加尴尬。为了帮她挽回面子，我大声说："女士，很抱歉我的笑让你难堪了。"这让她在周围人面前挽回了面子。她理解我"这是为了大家好"，所以变得极为亲切。一分钟之后，她向我道了歉，而我得到了所有想要的数据，一般情况下，要获得这些数据可是要颇费周折的。

我的一位老师过去常说："友善害人于无形。"这是非常有道理的一句话。对人友善是构建共识的快速方法，是实现说服和影响的5个基本原则之一。

通过友善与共识影响他人的一种方法是提出问题，然后让他们选择你想要的结果。例如，在一次团队工作中，我就被影响了，继而做了一件本不想做的事情。团队负责人很有魅力也很友好，是那种具有"魅力因素"的人，他和每个人都能谈得来。他走到我跟前说："克里斯，我想和你单独谈谈。在这个小项目中，我需要一个好帮手，他必须积极能干，有上进心。你是再合适不过的人选了，但我不想武断，你觉得呢？"

面对这样的恭维，我很激动，而且感觉自己很"重要"，所以回答说："我绝对是个很有上进心的人。有什么需要做的，尽管说。"

团队负责人继续说道："我认为榜样的力量是无穷的，而且认为你就具备领导才能，问题是团队中的有些人做不到，所以需要一个能手来告诉他们怎样做。"

在对话结束前，他成功地将他的想法变成了我的，令我不可能畏缩。这次的说服非常成功。

### 6.1.3 保持自身和环境一致

对自身和周边环境保持警觉或者说感觉敏锐，是一种洞察目标和自身状况的能力，它会告诉你你是否在朝着正确的方向前行。

第5章中讨论的很多原则也适用于说服战术。观察目标的肢体语言和面部表情，就能够大致知道你对其产生的影响。

要想真正掌握影响和说服的艺术，必须成为观察和倾听大师。加拿大阿尔伯塔大学的认知神经心理学家克里斯·韦斯特伯里（Chris Westbury）估计，人类的大脑在处理信息时每秒钟能够计算2亿亿次。这些计算会以面部表情、微表情、手势、姿势、语调、眨眼、呼吸频率、说话方式及无声语言表达等各种不同的方式呈现。掌握影响战术就是要敏锐地把握自身以及他人的这些细微呈现。

在接受艾克曼博士的微表情训练后，我发现自己更擅于观察了。随后我发现自己对周边以及自身的变化更加敏感。当感觉到脸上出现某种表情时，我就能够分析出它对别人产生的影响。这种对自我以及周边环境的认知，是我生命中最重要的体验之一。

NLP专家提倡在尝试影响他人时尽量减少内心活动。如果你在靠近目标时想着下一步进攻、终极目的或者怎样解决潜在的不利因素，这些内心活动会使你对周边的变化反应迟钝。成为敏锐的观察者需要付出大量的努力，但是这些付出都是值得的。

### 6.1.4 不要疯狂，要灵活应变

这里说的不要疯狂和灵活应变是什么意思呢？“疯狂”的一种广为流传的定义是“不断重复做同样的事，期待不同的结果”。愿意并且能够保持灵活应变是说服策略的关键之一。

可以从物理事物的角度来思考灵活性。如果任务是说服或者弯曲某物，你会选择一根柳树枝还是一根钢条呢？大部分人会选择柳树枝，因为它有弹性，很容易弯曲，任务可以完成。尝试说服顽固不化的人是不会成功的，同样，如果自己不能灵活应变也不能成功说服他人。

很多时候，审计工作不会按照计划进行。一名优秀的社会工程人员能够顺势而为，按照需要调整目的和方法。这和之前所说的预先计划并不矛盾，相反，恰恰说明了当事情不能按照计划进行时不要死板，这样才能在调整中继续前进，目的才能最终实现。

人们对疯狂的人的看法与目标对不能灵活应变的社会工程人员的看法如出一辙。如果社会工程人员不能灵活应变，其行为会显得不合情理，他也很有可能永远无法实现目标。

### 6.1.5 内省

这里说的内省不是禅宗所说的冥想，而是要理解自己的情感。情感几乎控制着你所做的每一

件事情，目标的所作所为亦受情感控制。了解你的情感并且不断内省，会为你成长为一名高效的社会工程人员铺就平坦之路。

回到前面你和抽烟的朋友的例子。如果你从心底里怨恨抽烟的人，会影响你的所作所为。它会在你的言语或行为上表露出来，从而断送说服的可能性。在某些事情上，你可能绝对不会让步，注意这些事情及你当时的情感有助于为影响目标开辟光明大道。

这5项基本原则是理解“影响和说服”的关键。“创建一个环境，使得目标想要按照你的要求去做”就是说服的目的，这5项原则有助于你创建那个环境。下一节将分析社会工程人员是怎样应用这些基本原则的。

## 6.2　影响战术

前面提到过，社会工程人员必须练习说服的技巧，直至它变成日常习惯的一部分。这并不是说他们必须影响每件事中的每个人，但是能够随心所欲地使用这一技巧是杰出社会工程人员的优良品质。

影响和说服的很多方面都可以为你所用，并且可以轻松地应用于社会工程审计中。其他一些方面可能使用起来并不容易，但是在“影响”领域里具有重要的位置。下面将介绍与影响相关的8种不同的战术，它们经常被媒体、政客、政府、骗子、诈骗犯及社会工程人员所使用。

下面各小节介绍了这8种战术，我们会详细分析它们在社会工程领域的应用，同时也会涵盖其在其他领域的应用情况。

### 6.2.1　回报

回报是一种固有的期望，指的是在他人对你好的时候你会给予友善的回应。举个简单的例子：当你走进一幢大楼的时候，如果有人为你开门，他会期望你对此表示感谢并且希望你报之以李，能为他打开下一扇门。

回报的规则很重要，因为报之以李通常是在无意识的情况下完成的。理解这一层含义会让你在社会工程中更好地运用它。在具体分析之前，先讲几个经常运用回报方法的具体例子。

- 制药公司会给每位医生（是的，每位医生）送10 000到15 000美元的“礼物”，包括晚餐、书籍、计算机、帽子、衣服或者其他物品，这些物品上都印有医药公司的标志。在医生选择一种药品给予支持或购买的时候，你认为他们更可能选择哪家公司的呢？
- 政客会被几近相同的方式所影响。众所周知，大多数情况下，政客或说客会更支持那些曾帮助他们竞选的人。
- 回报也经常应用于商业活动，特别是在和合同相关的事情上。也许销售人员会为宴请客户

埋单，其后他们会要求对方在合同上有所让步。客户有时不得不让步。

- 有个同事曾在你请假的时候替你代班。现在他请你帮忙，可是你已经有安排了，此时你通常会调整计划以答应他的请求。

这些都是回报的例子。社会学家阿尔文·古尔德纳（Alvin Gouldner）写了一篇论文，题目是The Norm of Reciprocity，内容详见http://media.pfeiffer.edu/lridener/courses/normrecp.html。其中有这样一段话。

> 具体说来，我认为通常情况下回报的规则包括两个相关的最小要求：(1)人们会帮助那些帮助过他们的人；(2)人们不会伤害那些曾经帮助过他们的人。基本上，人们可把回报规则想象成一个维度，在所有价值系统中都可以找到，具体表现为道德准则中普遍存在的一个“重要元素”。

根据古尔德纳教授的研究，基本上在各种不同的文化背景中回报都能够起作用。应用在正确的场景中时，回报很难被拒绝。

可以将回报设想为一个过程，如图6-1所示。

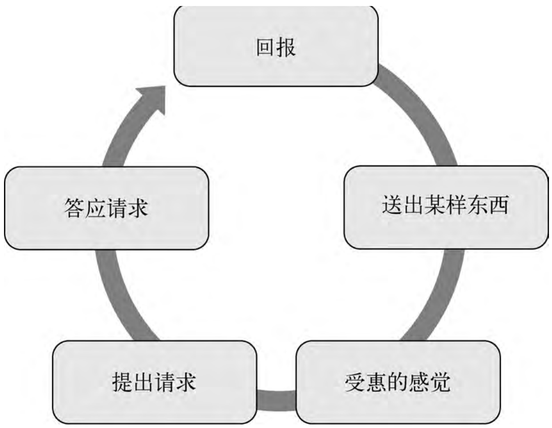



图6-1　回报的循环过程

下面展开介绍这个过程中的一些关键点。

### 1. 送出某样东西

你送出的不能是完全没有用的东西，必须是有价值的东西。假设送出的是一本精装小说，但是接收方不收集或阅读该语种的书，这样做就徒劳无功。

送出的可以是一项服务、一件物品、有价值的信息、帮助或者任何接收方认为有价值的东西，甚至简单到为对方开门或者拣起一件掉落的物品。一些销售组织推崇这一方法，却因送出的东西

毫无价值而功亏一篑。设想你参加一次展销会，每个参展商都有礼品送出。如果发现有一家只是送出廉价的笔，你会毫不犹豫地走开。下一家送出的礼品是谜题类的游戏，很吸引眼球，你拿起它玩了几分钟，然后销售员走过来问道："需要提示吗？"在演示通关技巧之后，他会问你是否有时间看看他们提供的精彩服务。

这种情况下，你怎么忍心拒绝呢？你拿到了一个有趣的游戏并且获得了免费提示，现在他只需要一分钟来向你介绍服务。这是一种很完美的布局技巧。

### 2. 制造受惠的感觉

对接收者来说，礼物的价值越高或者越意外，受惠的感觉越强烈。

重要的是不要将礼物用在明显的操纵战术中。不要这样说："我给你这么好的礼物，你欠我的。"甚至这样想都会让对方失去受惠的感觉。"礼物"必须完全免费，必须于对方具有很高的价值。

比如，美国人道协会将量身定制的邮寄标签作为免费的礼物送出。它们看起来很漂亮并且质量也不错，而且没有任何附加条件，人们可将它用于节日贺卡或者个人信件。标签上有你的签名，几个月之后你可能会接到电话，对方希望你捐款支持本地的人道协会。接收者的责任感是很强烈的，多少都会贡献一些。

再看另外一个例子，《财富》杂志为大学教授提供免费的期刊，在不附带任何条件的情况下，供其教学使用。

这样的例子有很多。另一方面，很多公司误认为下面的物品是好的礼物：

- 美丽夺目的公司宣传册；
- 无用的小玩具；
- 关于你的公司或产品的销售资料。

这些东西不会让人产生受惠的感觉，接收者必须认可"礼物"有价值才行。另一种构建真实受惠感的"礼物"就是信息。从某种角度来说，为对方提供一条有价值的、会带来好处或者有用的信息会比实际的礼物更能引起对方的兴趣。

### 3. 提出请求

一次在进大楼的时候，我看见一个貌似"老板"的人从车中走出来，车停在了"CFO专用"的车位上。他正在打电话，看起来不是很高兴，我隐约听到他告诉别人自己有一种糟糕的感觉，因为他要进去开除一些人。从他的语气中可以判断出他是在与妻子或者女朋友通话，而且他对这项工作任务比较排斥。

我经过他的身边走向前台，在这过程中我发现前台的女孩正在玩扫雷游戏。当我走近时，她

以标准的口吻问："请问有什么可以帮您？"她脸上有一种无聊的表情，似乎心不在焉。我说："嗨，我是来开会的，你的老板马上要进来，并且心情很不好……"此时我压低了声音，拿着一个文件夹站在那里。几秒钟后老板走进门，我大声说："多谢你的帮助。"

她看着我说："请稍等一下，先生。"然后对她的老板说："早上好，史密斯先生，这边有您一些东西。"然后在他经过的时候递给他一小叠纸。

在老板进入办公室后，她多次感谢我。她很清楚我刚才帮了她大忙，因为我提供的信息对她来说是无价的，所以接下来我的话就变得很有分量："我需要你帮个忙。我想见见人力资源部经理，你能让我尽快见到她吗？"

她将我带进经理的办公室，并且在门口介绍我是"她的朋友"。几分钟内我的计划就成功了，这都是回报带来的好处。

作为社会工程人员，寻找适当的小机会送出一些信息，会突显你在接收者眼中的价值，更重要的是让接收者感激你。

仔细观察周边环境，看看能为目标做些什么事情，让他们感激你。谨记，不需要是什么一鸣惊人的事情，只要对他们有价值即可。要谨记的诀窍就是不要让对方感觉"不寻常"，紧盯战术或者迫不及待的行为只会带来厌恶感。要很自然地应用这些原则。

自然的含义就是可以在日常生活中开始应用这些原则。为人们开门、保持礼貌并寻找可能帮助他人的机会。这些行为会成为你的第二天性，这样在社会工程审计活动中做起来就很自然。

回报是一个强大的影响战术，下面讨论的两个原则与其密切相关。

### 6.2.2 义务

义务就是基于社会、法律和道德要求，以及责任、合约或者承诺，人们认为必须做某件事。在社会工程中，义务与回报紧密相关但又不限于回报。如果你为别人开了外面的门，对方通常会为你打开里面的门，义务有时就是这样简单。不过义务也可以扩展到别人向你提供一些私人信息，因为你让对方觉得这样做是他们的义务。当目标是客户服务人员时，通常可从义务入手进行攻击。

也可以简单地通过高明的称赞来施行义务战术。例如，先称赞某个人，然后提出一个请求。如果你是新手或者经验不足，很容易误用这种技术，会让目标觉得你很虚伪，引起其警觉，从而适得其反。但是如果运用得当的话，会为信息收集带来莫大的好处。

这里举一个恭维误用的例子，比如说："哇，你的眼睛好漂亮啊！我能进你们的服务器机房吗？"这很愚蠢，不是吗？所以一定要将你的方法大声说出来，并分析其效果。如果感觉这一赞许没什么价值，就不要用了。

如果会话采用的是下面这种方式，就是一种恰到好处的称赞。

在走近前台的时候，你看到几张小孩在迪斯尼乐园游玩的照片。在介绍自己后，你说："那是你的小孩吗？好可爱啊！"不管他们是前台的小孩还是她的侄子，听到这样的称赞，她都会很高兴的。你还可以接着说："我也有几个孩子。他们让我们保持年轻，对吧？"

"这是我的两个孩子。不敢说让我年轻，但确实让我筋疲力尽。"她轻声笑着说。

"我还没带孩子们去过迪斯尼呢，你认为那么大的小孩喜欢那里吗？"我说。

"当然，喜欢得不得了。"前台说，"只要我女儿和她爸爸在一起，就会很开心。"

"哈哈，我的小公主也是。"我回答道，"我可以站在这儿聊一天关于孩子的故事，但是能否请你帮个忙？我上周打电话过来和某人沟通过关于新的人力资源软件包的事情，我答应将资料拿过来给她，但是我忘记她的名字了。真不好意思。"

"哦，那可能是史密斯夫人，"前台开始提供信息，"这些事都是她处理。"

"你真是帮大忙了。我欠你一个人情。谢谢你。"

这种类型的恭维会比较有用，能够打开目标的话匣子，使得他们更容易被影响。

黄金法则（己所不欲，勿施于人）是创造"义务"的一个重要原则。对别人友好，给他们需要的东西，甚至是简单的赞美，都能使他们觉得有义务帮你。

心理学家史蒂夫·巴塞特（Steve Bressert）在他的文章Persuasion and How to Influence Others中阐明了这一点："根据美国伤残老兵组织的反馈，通过简单的邮寄方式发出捐赠请求会有18%的成功率。如果其中包含一个小礼物，例如个性化的地址标签，则几乎可以将成功率翻倍，达到35%。'因为你给我寄了有用的地址标签，我会回报以小额捐赠。'"

如果想亲自证明这个原则的强大威力，可以尝试下面这个简单的练习。即使一个小问题也能制造"义务"。下一次有人在谈话中问你问题时，不要回答，保持沉默或者忽略这一问题继续谈话。你会注意到这很尴尬，抛出问题就能让对方觉得有回答的"义务"。仅仅是问目标一个问题就能产生神奇的效果。

如果你的第一步给人以期待下一步的感觉，那么他们会有强烈的满足你的期许的义务感。当与你交流的人期待一个结果时，你给出的答案会让他们极其想投桃报李。

再举个例子，你可以送目标公司CFO一个科技产品，也许是装有恶意软件的iPod。他得到礼物后有"义务"接到计算机上使用。我见过一种成功的攻击方式，社会工程人员给CFO或CEO送了一个礼物，里面有一个卡片，上面写着："小小礼物不成敬意。还请您登录www.products.com浏览一下我们的产品，并且在www.products.com/catalog.pdf下载产品目录的PDF文件。我会在下周致电交流。"

这个方法屡试不爽。

### 6.2.3 让步

让步或者让步的行为，可以定义为“承认或认可”或者“屈从的行为”。让步经常用在社会工程场景中，是对人们回报天性的利用。人类似乎有一种天性，想要“投桃报李”。社会工程人员可以使用这种“交换”思维，或者“礼尚往来”原则。

下面列出了关于让步及其正确使用的基本原则。

- **表明你让步** 明确让对方知晓你何时以及做出何种让步，这会让对方很难不回报。可以说，这会取得某种平衡，因为在宣布让步的时候你不想自吹自擂，但是简单地说“好吧，我给你这个”或者是“好，我妥协”足以显示你愿意让步。
- **要求和定义回报** 可以在开始时植入回报的种子，这会增加你获得回报的机会。一种简单的植入方式是通过非语言交流显示你的灵活性，同时做一个好的倾听者。在让目标感觉需要回报的时候，这种细节处理能够产生极大的效果。
- **视情况做出让步** 在信任度很低的时候，或者当你想要发出其他让步信号的时候，可以做一些“没有风险”的让步。这不是那种需要摆出“现在你要为我做些事”态度的让步。通过放弃目标想要或者需要的某样东西，并且不提出相反的要求，你和目标的关系会更加融洽。
- **分批做出让步** 回报的想法在我们的头脑中根深蒂固。大部分人会觉得在得到别人的帮助后，他们之间就存在一种社会契约，自己最终是要回报对方的。类似地，如果某人做出了让步，例如在协商或者达成交易合约的时候，那么对方会本能地感觉有义务“返回”一些。因为这是事实，所以所有的让步不必一次到位。可以进行“分批”让步，可以这里让一点那里让一点，久而久之，目标也会不断回报的。

销售人员、谈判代表和社会工程人员每天都在使用让步技巧。一个成功的社会工程人员可以使用或者利用这种本能，这样不仅可以抵御对方的操纵，也可以尝试取得对局面的完全掌控。让步和回报技巧能够和本书中讨论的其他社会工程技巧完美结合。

我们可以用电话销售员号召捐款的示例来阐明有多少人会被让步策略影响。他们一开始提出一个人们会拒绝的大数量请求，随后采用让步技巧，将数目减少，这就比大额捐款容易接受多了。

大数量请求：“您能为我们的慈善活动捐款200美元吗？”

响应者：“不行。”

小数量请求：“哦，先生，不好意思，我完全理解。那么您能捐20美元吗？”

不提防这种技术的人会感觉一下子轻松了，他们会觉得仅仅拿出20美元就可以了，而不是一开始提出的200美元。

另外一个极好的例子出现在大卫·希尔（David Hill）的文章中（详见http://ezinearticles.com/?How-to-Negotiate-the-Salary-Using-the-Power-of-the-Norm-of-Reciprocity&id=2449465）。

> 大部分讨价还价的场景中都能体现出这一准则的强大威力。假设买家和卖家正在就汽车的价格讨价还价。卖家的初始出价为24 000美元，买家觉得难以接受，还价15 000美元。然后卖家将售价降到20 000美元，此时他做出了让步。这种情况下，买家很可能提高他的出价，也许会提到17 000美元。买家觉得有必要提价的原因就是回报准则。这种准则要求买家对卖家的让步行为做出让步。

和我们目前为止讨论的大部分原则一样，让步必须对接受方具有价值。不能让出一些只对自己有用的东西，否则不会得到应有的回报。

作为社会工程人员，如果让步会导致丢脸、丧失共识或者失去有利位置，也是得不偿失的。让步和你与目标的关系之间必须实现微妙的平衡，找到平衡点就意味着成功了一半。找到它，让步就会成为你手中的一件利器。

### 6.2.4　稀缺

如果物品或者机会比较稀缺或者难得，人们通常会觉得其更有吸引力。这也是我们经常在报纸和电台广告中看到或听到“最后一天”、“限时提供”、“仅售三天”以及“关门甩货”等信息的原因，这会诱使人们尽快去购买这些“以后再也不会有”的产品。

销售场景中使用稀缺概念的最典型语句就是“尽快行动！限时特供！”。还有一些也很常见，比如“最先打入电话的X位将获得免费的附件”，或者为流行产品故意制造一个短缺的假象。最近，任天堂Wii游戏机的销售就应用了这一策略。Gamasutra游戏网站的专栏作家贾森·多布森（Jason Dobson）说：“但是我认为任天堂有意制造了供应短缺的假象，他们想在财年内卖出更多设备。新财年起始于4月1日，我认为供应会很充足。”（详见www.gamasutra.com/php-bin/news_index.php?story=13297。）

在我居住的地方，一家汽车经销商在某周四发布广告说，由于新车到货他们将会处理XX辆车，价格极低而且有些车型不会再生产，该周末是见证一段汽车销售历史的最后机会。

那个周末的销量就像乘坐了火箭，那么空仓销售结束了吗？没有，那个广告持续播放了三个多月，每周四都会出现。我经常奇怪人们为什么就不明白，但是经销商确实通过这种方法卖出了很多汽车。

如果应用了稀缺策略，社会事件经常会引起更多的关注。在这种情况下，意识到参加这些社会活动的好处经常会不断点燃人们的热情。广告策略中，关键点就是宣告最后的演唱会门票即将售罄，这会收到很好的效果。

很多受欢迎的餐馆会关闭一部分区域，造成更加繁忙的假象。这种极度受欢迎的现象会增强人们在那边订餐的欲望。如果要看一个真实的利用稀缺策略宣传的广告，可以移步www.social-engineer.org/wiki/archives/Scarcity/Scarcity-Advertisment.html。

这个广告中有4个主要部分都使用了稀缺策略：

- 活动是限制参加人数的；
- 申请是不向公众开放的，仅部分人可以申请；
- 发起人有限且经过精心挑选；
- 只有那些被选中的幸运儿才能得到免费电子书。

所有这些点都应用了稀缺策略，使得想参加的人感觉困难重重，认为只有少数精英、杰出人士才能有机会踏入那神圣的殿堂。

经济学的基础就是对那些可供选择的资源进行分配。这种分配由待分配物的稀缺性驱动，资源越稀少，物品的感知价值就越高。这也是黄金比食盐值钱得多，而食盐又比黏土值钱得多的原因。

同样，稀缺也经常应用于日常活动中。通过提高个人拥有的某物的价值，稀缺也和社交场景建立了联系。例如，有人貌似一直很忙，很少有自由支配的时间。这种行为给了他一个借口，不能和其有义务陪伴的人经常在一起，同时使得他们一起度过的时光看起来更宝贵。

也可以通过使用稀缺的方法操纵人们的注意力。很多人抱怨他们在逛商店的时候销售人员一直跟着，甚至打扰了他们。但是当销售人员对其不理不睬时，他们又会觉得被冷落了。总体上来说，人们渴望得到那些难以企及的东西，因为这些东西看起来更有价值。别人的关注亦遵循这一规律。

社会工程场景中也经常会用到稀缺的方法，以便在需要作出决策的情况下制造一种紧急的感觉。这种紧急经常导致决策过程被操纵，使得社会工程人员能够控制受害者需要的信息。这个过程中通常会使用权威和稀缺的方法。例如，可以这样说："首席财务官史密斯先生在周末出发度长假前打电话给我，要我过来解决他的邮箱问题。他说已经被邮箱崩溃的事情折腾得精疲力竭，希望能够在周一前修好。"此时的情况就是紧张而且稀缺，无法与首席财务官通话，而且时间很紧张。

将稀缺与其他方法一起使用，也会使得攻击更加致命。总之，稀缺制造出一种欲望，而欲望导致人们做出一些事后可能会后悔的决定。

我最近亲身经历的一件事也证明了这一点。有一天，一辆后面带有冷冻室的卡车停在了我的私人车道上。车上下来一位穿着得体的年轻人，他走近我的妻子，说他是一位鲜肉销售员，为客户送完肉回办公室的路上正好经过这里，看到我的妻子在院子忙碌就停下来了。他开始说最近商

店里的肉价在不断上涨，所有东西都比以前贵了不少。我的妻子是一位价格敏感的购物者，所以这就拉近了关系。而且他带有令人愉快的南方口音，尊敬的“夫人”称呼一直挂在嘴上。

在几分钟的交谈后，她脱口而出一个通常能够令大部分销售员人中止说话的问题：“你们卖多少钱呢？”

他没有丝毫停顿，立刻说道：“你瞧，我们的肉一直都是400美元一盒，但这是最后一盒了。我非常想在回办公室之前将所有的肉销售一空，同时你也能买到高质量的肉。”

不是吧，最后一盒！他之前告诉过她，他每两个月才会从这边走一趟。欲望已经被燃起，但我的妻子也不是笨蛋，她知道自己被操纵了，于是让他等一会儿，然后过来找我了。

他滔滔不绝地说着，三句话不离最后一盒以及很少来这边。当然，对于怎样才能不落入这种战术圈套，大家可以参考这个案例。问题是他们已经聊了不少时间了。他看到我们屋子外面有一个烧烤架，就知道我喜欢在外面烧烤，而他具有这方面的专长。他开始谈论肉的品质，并且将他盒子中的肉和餐馆中的肉进行对比。

很多人会轻易被他的推销技巧说服。“如果这是他的最后一盒呢？”“他是对的，这比出去吃要便宜很多。”“他开车送过来……我都不需要开车到商店。”

相反，我拿出计算器，问他最后两盒肉的重量，计算出单价，同时问妻子通常餐馆或者商店中肋骨肉多少钱一磅。她报出来的价格每磅要低3元，我沉默不语。现在他的表情看起来有点混乱，他急着挽回面子，一下子将价格降低了150美元。我再次计算，他的肉每磅还要贵0.5美元。

他开始谈论肉的品质、方便性以及这0.5美元物有所值的理由。我改变了一下姿势和位置，离他远一些表示我不感兴趣。在我没有说一句话的情况下，他结束了滔滔不绝的生意经，将价格又降了50美元。我告诉他：“抱歉，我认为价格还是高了。”

然后他犯了典型的错误，暴露出他声称的稀缺是误导——他作出了更多的让步。“如果将两盒一起买去，你能出多少钱？”

“100美元的话还有可能。”

“如果你出125美元的话，就成交。”

请注意，之前他的价格是400美元每盒，而且这是最后两盒，他两三个月才从这边走一趟。这次的砍价可真够狠的，但是相反，我没有买就让他走了。

这个故事给社会工程人员的教训就是，要想“稀缺”发挥作用，要么这种稀缺是真的，要么就要坚持你的观点，让它看起来是真的。

对于真正需要的物品，人们会高估其价值。一个反面例子就是汽油公司在卡特里娜飓风后

会提高燃油的价格。他们声称飓风的破坏使燃油出现短缺，导致了油价的大幅提高。当然，如果情况属实的话，燃料价格会比声称的更高，但是这只不过是利用稀缺借口赚钱的反面例子。同时，当BP公司的错误导致数百万加仑的石油污染墨西哥湾，使生态环境受到破坏时，油价并未因原油供应短缺而飞涨，反而有所下降。这是怎么回事？我并不想在这里讨论这个问题，但是它证明了要想稀缺原理发挥作用，它必须是可信的。石油公司失败于此，社会工程人员也可能重蹈其覆辙。

从社会工程人员的角度来看，如果限制很多或者机会难得，价值也就越高。如果信息是私有的、受限制的且难以得到，并且你愿意与他人分享，你在他们眼中就极具价值。

社会工程人员可以在利用信息的稀缺性时说："我不能说这个，但是……"也可以说："我不确定你是否听过这个消息，但是我听说……"以严肃的语调说出这样的句子意味着信息很难得。

### 6.2.5 权威

人们更愿意听从他们眼中的权威人士的指导或建议。要找到足够自信、敢于直接质疑权威的人是很难的，如果权威是他的直接领导或者双方面对面的时候，质疑就更加困难了。

例如，孩子被教导要听大人的话，要听老师、辅导员、神父、保姆的话，因为对他们来说这些人都是权威。通常来讲，质疑权威会被认为是不敬，谦卑的服从则会受到褒奖。在成人的生活中存在同样的原则，我们从小就被教导要尊重权威人物，不要质疑规定或者权威人士的命令。

不幸的是，这一原则让很多孩子落入施虐者和性骚扰者手中。当然，结果并不是这一个原因造成的，但是那些拐骗孩子的人知道孩子从小就是被这样教育的，所以经常寻找那些乖巧的孩子。同样，恶意社会工程人员使用这个原则操纵他们的目标，利用他们的行动或不作为达到入侵的目的。

了解权威在社会工程活动中的应用很重要。德国社会学家和政治经济学家马克斯·韦伯（Max Weber）对权威进行了定义和分类，我将这一分类应用到了社会工程领域。

#### 1. 法律权威

法律权威的基础是政府和法律。执法人员或者你所在国家、区域和机构的行政管理人员就具有这种权威。

作为社会工程人员，伪装成执法人员或者其他政府官员通常是违法的，不过伪装成保安、银行保安或者其他类型的具有执行权威的人就没问题，也常用于社会工程实践。

在英国广播公司《骗术真相》的一期节目中，保罗·威尔森和同伴装扮成收钱的警卫。如果某人穿上足以以假乱真的制服，并且在行动上和平常处于这一权威位置的人一样，目标很少会质疑这种冒名顶替者。装扮成权威人物是社会工程人员混入公司的主要手段。

另外一种有效的策略就是装扮成律师，前来提取特定的信息。装扮成大众畏惧或者尊敬的角色可以获得某种权威。

### 2. 组织权威

简单来说，组织权威是通过组织的方式定义的权威，通常涉及管理层级。在组织中具有高层级和权力的人比低层级的人获得的权力及信息多。

在社会工程审计中，顾问会模仿首席信息官或其他具有组织权威的人，他们可以利用赋予的权威从前台或者其他员工那里获取口令等信息。

美国司法部的乔纳森·鲁希（Jonathan J. Rusch）写过一篇文章，名为The‘Social Engineer’of the Internet Fraud，其中说道：“在适当的情况下，人们更可能对来自权威的主张作出快速的反应，即使这种所谓的权威根本未露面。”（详见www.isoc.org/inet99/proceedings/3g/3g_2.htm。）

人们也会通过其他方式来应用这一策略，如假扮成获得首席财务官授权或受其指派的人，而不是其本人。由权威人士的名称和头衔带来的权威使得攻击者在目标眼中具有足够的权力。

鲁希引用了罗伯特·恰尔迪尼所著的《影响力》（*Influence*，1993）一书中记录的一个实验，实验显示来自3家不同医院的22个检查站的95%的护士愿意给病人注射一种危险的药物，仅仅是因为接到一个素未谋面的据称是研究者的电话。

实验清晰地显示了，基于命令或来自权威的指示，人们会不顾自己的正确判断做出特定的行为。这种类型的权威可以并且经常被用来入侵公司，拿走具有价值的数据。

### 3. 社会权威

社会权威指的是社会团体中的“天生领导者”。社会团体中可能包括同事、大学同学或其他聚集到一起的人。

在《影响力》一书中，恰尔迪尼写道：“自动对权威作出反应时，人们往往是对权威的符号作出反应，而不是其本身。”

要想产生社会权威，不需要用很多时间和结构来定义一个权威人物。无论是何场景，都有明显的证据，即人们会受一小群采取同样行动的人的影响，这就是社会权威。

在社会工程中可以利用社会权威询问或者给目标施压，以得到特定的信息。如果目标拒绝就会受到小组领导者的排斥，导致他在整个小组中被边缘化。服从领导者的社会权威会让人们觉得更加有利。

攻击者如果想要成功地利用社会权威，可以明示或暗示前面有人或者小组许可这样的行为。“昨天首席财务官让我过来解决这个问题，乔检查了我的所有证件让我过去了，文件有记录吗？”

这句话中就利用了几种形式的权威。

如果毫无防备地顺从权威，就会不顾现实地服从于权威符号。在西方国家，三种权威符号特别有效。可以用下面三种符号之一来获得别人的顺从（没有其他证据表明他是权威）。

- 头衔
- 衣服
- 汽车

在一次对埃伦·兰格博士（哈佛大学心理学家，研究说服和影响力）的采访中，在“毫无防备”方面她说了很多。她说人们在日常工作中不会考虑很多，换句话说就是有点机械化。这种情况下，对权威角色的滥用就非常危险。感知的权威可以让他人没有限制地机械响应。详见www.social-engineer.org/episode-007-using-persuasion-on-the-mindless-masses。

通过得体的衣着、肢体语言甚至一张假的名片，社会工程人员就可以冒充权威，让他们的目标自发响应。

社会工程人员还可以利用这里没有列出的其他权威方式，但是这些是最常用的。权威在影响他人方面是一个强有力的武器，通过一些信息收集和推理，社会工程人员就能有效地假扮成权威，从而取得优势地位。

### 6.2.6 承诺和一致性

人们欣赏遵守承诺的人，也希望自己言行一致。通常人们会在言语、态度和行为上保持一致。言行一致降低了信息再处理的必要性，并且为作出复杂的决策提供了捷径。

直觉（就是根据以往的经验判断某一行为的好坏与对错）通常会指出所作的决定可能与以往的感觉和信念相矛盾。这些信号让你感觉自己是被逼同意的，内心其实并不认同。

直觉也会在作出承诺时产生。它表明你并不确定自己的承诺是否正确。你可以扪心自问：“若时光倒转，根据已知信息，我是否会作出相同的承诺？”

在分析社会工程人员如何利用言行一致来获得他人的承诺之前，我们先看3个有关这方面的例子，这会有助于理解。

- **营销** 公司通常会花费额外的资金以争取更大的市场份额。这并不会增加回报，但是他们相信最终会有利可图，所以值得投入。可口可乐和百事可乐过去几十年在营销上的明争暗斗就是一个很好的例子，然而商业宣传并不会让人们由喜欢百事可乐变成喜欢可口可乐。因为两家公司都“承诺”决不让步，所以当其中一家推出新产品或者展开新的市场宣传时，另一家会立刻跟进。
- **拍卖** 类似eBay等在线拍卖网站越来越流行，他们对承诺原则的应用更加明显。人们

在出价时会感觉作出了一定程度的承诺，如果有人出价更高，他们就会继续跟进。因为承诺，他们偶尔甚至会将价格抬高到自己都不满意的程度。罗伯特・坎普（Robert Campeau）收购布鲁明代尔百货公司（Bloomingdales）就是一个典型的例子，在原有的价值之上他多花了6亿美元。《理性交易》（*Negotiating Rationally*）的作者马克斯・巴泽曼（Max Bazerman）引用《华尔街日报》记者的文章说："我们已经不再基于价格进行交易，而是基于自我意识……"

- **嘉年华及赌场等**　任何时候，只要涉及赌博或赌场，就存在承诺，他们会用遵守承诺说服人们参与赌博。瑞安・希利（Ryan Healy）是一位在线市场顾问，他在专栏中写过一个带女儿去马戏团的故事，详见www.ryanhealy.com/commitment-and-consistency/。他花了44美元买票，5美元停车，开了40分钟车到达马戏团，因为他承诺过要带女儿去看马戏。女儿要吃棉花糖，他答应了并给了她5美元。棉花糖不会高于这个价吧？当卖糖的人过来说每袋要12美元的时候，他怎么能违背承诺呢？他不能，因而最终花12美元买了一袋棉花糖。

这种虚假的一致性被定义为根据以往的经验或期望所应有的预期。那些经验或者期望会驱使目标采取导致入侵的行动。例如当技术支持人员过来时，按照预期他会进入服务器机房，那个要求与之前的经验和期望一致。当伪装者要求进入服务器机房时，他能够得到允许，因为这和目标的预期一致。

要使大部分人采取特定的行动、透露信息或者泄露秘密，承诺和言行一致可能是很大的影响要素。

社会工程人员武器库中应该有承诺和言行一致这一强大的武器。如果社会工程人员能够让目标做出一些小的承诺，那么扩大这个承诺也不是什么难事。

罗伯特・恰尔迪尼在《影响力》一书中这样写道：

> 使用承诺和言行一致操纵他人的关键在于初始承诺。也就是在作出承诺、明确立场之后，人们会更加愿意同意那些和他们初始承诺一致的要求。很多说服专家会尝试引诱对方选择一个初始立场，该立场与他们随后要求的行为一致。

希望采用承诺与言行一致原则的社会工程人员通常会让目标人物泄露一些通向最终目标的细微信息。通过让目标对象的行为与其已经说出的事情保持一致，攻击者可以让对象泄露更多的信息。

另一方面，攻击者的行为也必须与自己所说的保持一致。攻击者应该从小处着手，逐步扩大信息收集的范围。

举一个不现实的例子，攻击者不能一开始就询问核设施的发射码。这个要求肯定会被拒绝，此时攻击者剩下的选择就不多了，而且不能收回这一要求。不过，如果从小处开始，逐步扩大收

集信息的范围就会更加自然，对受骗者来说也不会显得太过突兀。

采用缓慢、渐进的方式会比较困难，因为社会工程人员通常会不耐烦，想要立刻拿到“密码”。如果能够保持冷静和风度，则更容易得偿所愿。清晰地定义每次审计采用的方式，甚至写下来，能够帮助你在审计时清晰地定义每一个目标，以及实现这些目标的步骤和方式。

如图6-2所示，我绘制了一个图表，显示社会工程人员如何采用可视化方法，设计出利用“承诺和言行一致”方法获取信息的具体步骤。




图6-2 清晰地定义目标有助于你获得信息承诺

如果让目标口头承诺采取特定的行为，就能够迫使目标掉入我们设定的圈套。恰尔迪尼说：“承诺和言行一致方法表明，作出决定时我们会承受来自他人和自身的压力，我们的行为必须要与此决定一致。依据以往的经验，你会在压力下作出或好或坏的决定。”

如果你曾经口头承诺妻子或配偶减肥，可能就会有这种感觉。这样的口头“承诺”会带来一系列的压力，最终需要承担一定的“义务”。

有时，要推翻自己的决定很难，甚至不可能。每个人在生活中都至少有过一次这样的经历，

最终会小声说："对不起，我改变主意了。"我们这样做的时候，一般都会低着头、面带愧疚，声音也会比较小，看上去很难过。为什么？我们未遵守自己的承诺，心理上有罪恶感。

即使是很小的、最不重要的承诺也会被利用。例如，律师常常会在电话里像下面这样说。

"嗨，今天好吗？"

你回答："很好。"

律师利用你的承诺说道："听到你这么说真好，因为有人需要你的帮助。"

现在你不能违背之前说出的话了，因为你仍旧"很好"而且承诺了。

这并不是说我们需要偏执到回答任何简单的问题都要担心被利用的地步，但是要注意即使作出了一个承诺也并不意味着必须承诺后面的所有事情。我曾经和一个家伙共事过，他能让别人唯命是从，并且还觉得那是他们自己的想法。其中的一个方法就是确保目标遵守诺言。

如果承诺和他在某些事情上达成一致，那就不可能不做，因为之前已经"答应"了，所以必须继续"答应"。这些承诺的最终结果就是按照他的设想去做，同意完成他所交待的工作。

注意，在某些事情上说"不"也是可以的，这样能够避免承诺所导致的灾难性后果。然而有时我们会觉得"拒绝"是一种原罪，需要祈祷多次才能被谅解。

在之前那个冻肉推销员的例子中，我的妻子表现出了强烈的自我防护意识。她知道自己可能会被这样一个"似乎很合算"的交易所操纵，所以进来找我，因为我"不受推销员欢迎"。

1972年，托马斯·莫里亚蒂博士（Dr. Thomas Moriarty）做的一个社会实验是显示承诺强大威力的范例。他让助手带着便携式收音机到海滩扮演"受害者"。助手坐在椅子上听收音机，10分钟之后起身去买饮料。

在他走开的时候，另一位助手扮演"罪犯"过来"窃取"收音机，没人知道他们在演戏。20个人中只有4个（只有20%）阻止小偷拿走收音机。

研究者在下一次的实验中略作调整。在"受害者"离开买饮料之前，他会请旁边晒日光浴的人帮他照看收音机。你认为这会发生怎样的变化？

现在20个人中会有19个站出来阻止小偷，有些人甚至不惜动用武力。为什么区别如此之大？这就是承诺和一致性的效果。研究者得到了旁边日光浴者的承诺，这使得他们遵守承诺。在我看来，这些令人震惊的统计数据充分体现了影响战术的强大威力。

社会工程人员能够有效地使用这一影响战术，促使目标承诺采取一些小的行动或表示认同，随后利用这个承诺扩大范围，从而产生更好的效果。

## 6.2.7 喜欢

人们喜欢那些喜欢自己的人。这个说法有点拗口，但却是一种真实的表述。深入理解这句话的含义有利于切实有效地掌握说服技巧。

当说“深入理解”的时候，我要说的是这个句子不像其表面看起来那么简单。

这并不是说喜欢你的人就会如你所愿。销售人员经常被告知，人们会购买自己喜欢的人销售的东西。这是真的，但不是重点。这也并不是说人们必须喜欢你，而是说你必须喜欢别人，他们才会喜欢你。

说起来容易做起来难，因为你不可能假装喜欢一个人。第5章中曾经讨论过，微笑和快乐很难作假。对想要影响的人，你必须深入理解、真诚关注。关心他人和他人的感受不是恶意社会工程人员的标准实践方式，因而他们经常依靠魅力。魅力可以在短时间内起作用，但是如果要达到长期影响的效果，喜欢就是一种更加实用并值得学习的技巧。

市场营销活动中广泛使用喜欢这一技巧。1990年，乔纳森·弗伦岑（Jonathan Frenzen）和哈利·戴维斯（Harry Davis）发表了一篇研究文章，标题为Purchasing Behavior in Embedded Markets，详见http://www.jstor.org/pss/2626820。文章中分析了为什么特百惠（Tupperware）系列产品会如此成功。他们的所有研究成果都证实了喜欢这一原则的重要性。

研究者总结说，大部人的购买原因在于让老婆高兴、帮助朋友，讨得他们的欢心。参加聚会时没有携带礼物会很尴尬！这种对失去欢心的恐惧驱使人们购买特百惠系列产品，而购买行为与实际需求关系不大。

其他调查和研究比较了人们在对待不同人群的“提示或建议”时的表现，这些人可能是朋友、陌生人，甚至是他们不喜欢的人。人们会倾向于接受朋友给出的“糟糕的建议”，而不会采纳不喜欢的人的“好建议”。

从社会工程的角度来看，喜欢这一技巧很有用。在社会工程过程中不仅需要赢得目标的喜欢和信任，同时必须对他们真正感兴趣。这就要说到第4章中讨论的伪装战术了。在进行伪装的时候，不仅要模仿角色的思想和观念，而是必须变成伪装的那个人。如果能做到这一点，让对方喜欢就会变得容易，你伪装的角色才能真正乐于帮助、喜欢或者协助对方。

对社会工程人员来说，喜欢的最后一个重要方面就是吸引力。人们倾向于“喜欢”那些有吸引力的人。这句话听起来很空，却是真理。一些严肃的心理学原则证明了这一点。

“美丽的就是好的。”这是1972年布尔沙伊德（Berscheid）、沃尔斯特（Walster）和迪翁（Dion）进行的一项研究的标题。这项研究揭示出一些意义深远的发现。参加者需要按照其中人物的吸引力强弱把3张照片分成高、中、低三档，还要仅仅基于照片，给人物的人格特质、总体幸福度和职业成就打分。

随后他们对打分进行汇总，并算出平均值，发现被认为具有吸引力的人在社会关系、职位、幸福度和成功率上都高于平均值。研究证明，人们倾向于将美丽和其他成功特性联系在一起，美丽会改变他们的观点和信任度。

这项研究是展示*月晕效应*现象的一个例子，某人的一种特质会影响或扩展到其他品质。研究证明，倾向于关注他人身上的优点会影响一个人的决定。详细内容参见http://www.social-engineer.org/wiki/archives/BlogPosts/BeautifulGood.pdf。

换句话说，如果别人认为你是美丽的，那么这个优点会影响他们对你的其他判断。这种月晕效应常用于市场营销。对于美丽的人所饮用、食用或穿着的物品，其他人会自动假设这些物品都不错，因而可能会想："如果这些人都在用的话，那一定不错。"

最近我在电视上看到的一则广告就是一个很好的证明。该广告以一种非常机智的方式嘲讽了营销手法。一位有吸引力的、衣着光鲜亮丽的年轻女性出现在画面中，说道："嗨，我就是公认的有吸引力的18~24岁的女孩。"

这是个天才的市场营销，片中出现的是一位真实的、有吸引力但又不是非常有吸引力的女性，我们在日常生活中就能够遇到。我们并不能真正判断出她的真实年龄，但是她的美丽让人认为她在18~24岁之间。

"你们可以理解我，因为我不属于哪个具体的种族。"

以上是另一个天才市场营销创意。她不是黑人、白人或北美土著人——我们看不出来，也许她是混血，这对很多种族都有吸引力，对大部分人来说也不会有冒犯的感觉。

"我出现在这则广告中，是因为市场研究表明，你们这些女孩喜欢我这样的女孩。"

她的美丽和自信让我们喜欢她，她穿着得体、语调优美，我们想要了解她。

随后镜头切换到她练习跆拳道、在啦啦队跳舞和赏花等不同场景。通过为观看者展示她做这些事情时的优美瞬间，我们注意到她的健康与活力，这些事也做得优雅到位。

"现在我要告诉你购买……"

接下来她开始推销护垫。这个商业广告太有创意了，因为广告者展示、使用并教导客户那些能勾起消费者购买欲望的方法。除了这些之外，这个广告中应用了喜欢的原则和月晕效应。

在了解喜欢的重要性之后，你会怎么做？为变成一个有吸引力的男人我花了不少工夫，更不用说要变成魅力十足的女性了。不断去看整容外科医生并不靠谱，那么社会工程人员有什么别的方式来运用喜欢这一原则呢？

了解你的目标。了解对他来说什么是可以或不可以接受的，他的穿着如何，他有何好恶。太多的珠宝、太浓的妆或者其他着装方式可能让目标无法接受。设想你在为一家诊所做审计，你伪

装成药品销售代表。你知道大部分销售代表穿西装、发型修饰得当，在外形、体味或行为方面都很自信，具有很多吸引人的特质，所以理成莫西干人[①]似的发型或者带个鼻环进去都会显得很突兀。

必须了解目标，这样才能成功装扮成目标期望的样子。服饰、发型及珠宝饰件等都不要让目标震惊、惊讶或厌恶。让他感觉自然，慢慢创造出让他喜欢你的气氛，再通过构建信任关系走向成功。

社会工程人员可以通过一些东西恭维目标。与目标在一起的时候，在适当的情况下，通过简单的恭维开始谈话会比较有效，例如："你的鞋子很漂亮啊，在哪里买的？"人们喜欢积极的肯定。一个人受到他人的恭维时，会倾向于继续谈话，以听到更多的肯定之言。这种恭维会增强目标的自我肯定，让他感觉你比其他人更了解他。

明尼苏达大学有一篇关于"肯定强化"的论文（详见www.cehd.umn.edu/ceed/publications/tipsheets/preschoolbehaviortipsheets/posrein.pdf），其中指出过多的正面肯定可能会起到负面效应。他们称之为*过度满足*，也就是"肯定"增强到过多的时候，会开始失去它的效应。要消除这种情况，可以通过问题来给出肯定。这种方法会增强正面的行为或态度，同时，提出关于他们自己的问题也会让他们感到高兴。

通过如下4步能够让人们喜欢你。

(1) 自信而积极的态度；
(2) 建立共识；
(3) 应用前面提到的方法，与目标和环境保持同步一致；
(4) 有效地进行沟通。

尼古拉斯·布斯曼（Nicholas Boothman）在他的*How to Make People Like You in 90 Seconds*一书中说道，人们会在遇见他人的头两秒内决定是否喜欢这个人，要改变第一印象是很困难的。他提出见面时要有好的态度。具备良好的表达能力和不同场景的沟通技巧会让你更受欢迎。你表现出来的就是他们感觉到的。面部表情、肢体语言及着装等必须反映良好和积极的态度。

布斯曼在他的书中提到一些受人欢迎的关键要素，包括询问很多问题、主动聆听及对别人说的话题感兴趣等，这样的行为有助于让人们喜欢你。

社会工程人员可能需要不断练习，如果能够变得令人喜欢，对审计之路将大有裨益。

### 6.2.8　共识或社会认同

社会认同是一种心理现象，发生于人们不能确定正确的行为模式的社会场景中。在看到他人以特定的方式行事或谈话时，你可以轻松判定这种行为是得当的。总体来说，社会影响会导致一

① 莫西干人是北美印第安人的一个分支，他们的头型称做莫西干头型。该发型兴起于20世纪70年代，形似马鬃。原来被认为颓废之人才蓄，也被认为是嬉皮士的标志。——译者注

个大的社会群体对正确或错误的判断达成一致。这种情况在人们进入不熟悉的场景时很常见，此时他们内心中没有一个参考框架，所以不知道怎样处理才是适当的，他们会照搬那些自己认为更了解这种情况、见多识广的人的行为。

罗伯特·恰尔迪尼博士在《影响力》一书中谈道："社会认同，即人们会做他人正在做的事情。例如，在一个实验中，一帮人在抬头看天，看热闹的人也会抬起头，看别人正在看什么。该实验一度中止，因为太多的人在看天，以致交通瘫痪。"

这里会列出一些社会认同的例子，以帮助读者明白它的强大以及检验自己是否曾利用过它。

社会认同广泛应用于市场营销中。发布高额销售数字就是对社会认同的一种利用，它向潜在的客户展示产品是多么流行。另一个例子是公司发布了带有其标识或口号的衬衫，此时穿着者会发出明确的认同信号。

社会认同不仅受大群体的影响，也受名人的影响。例如，当某名人使用某产品的时候，其他人会想拥有和该名人一样的优良特质，从而会使用同一款产品。

名人推荐效应的例子很多，近些年一家贝雷帽的主要供应商就让塞缪尔·杰克逊（Samuel L. Jackson）帮助推广他们的产品，如图6-3所示。




图6-3　塞缪尔·杰克逊戴着袋鼠（Kangol）帽

在市场活动中，公司宣传说他们的帽子是市场上最热销的，证据就是连塞缪尔·杰克逊先生都戴着它。

广告中经常会出现“销量最高”或者“热销产品”这样的字眼，通过这种方式让受众相信其得到了很多人的认同。

Media-Studies.ca网站有一篇利用社会认同影响目标的文章，详见www.media-studies.ca/articles/influence_ch4.htm。

> 实验发现，在播放幽默节目的时候，使用预先录制的笑声能够使听众笑得时间更长、更频繁，人们也会认为这个节目更有趣。而且一些证据表明，预先录制的笑声对拙劣的笑话最有效。问题是：为什么这样做会起作用，尤其是播放的笑声明显是假的？为了回答这个问题，恰尔迪尼给出了社会认同的原则：“我们确定什么事是正确的一种方法是看看其他人认为什么是正确的……如果在其他场合看到别人也做某事件，我们会更加坚信这样做是对的。”

和其他“影响力武器”一样，社会认同也是我们可以使用的一件利器：如果和周边人群的行为一致，我们就不会失礼。预先录制的笑声引起听众作出自动反应的事实表明，听觉暗示是一种强烈的刺激，因为它能在一定的意识层面影响我们。

另一个例子就是酒保或者其他人放置的“小费暗示瓶”，他们会放一些钱在瓶子里。当有人光顾时，暗示很明显：之前的很多人都给了小费，为什么你不给呢？这也很有效！

这个领域影响最深远、最杰出的研究之一来自克雷格博士（K. D. Craig），他毕生都在研究痛苦及其对人们的影响，为此他投入了毕生的精力。1978年他发表了一篇论文，题目是Social Modeling Influences on Sensory Decision Theory and Psychophysiological Indexes of Pain，详见www.ncbi.nlm.nih.gov/pubmed/690805?dopt=Abstract，他对其中的一个实验描述如下。

> 通常，若实验参与者接触了隐藏忍受或忍无可忍之感觉的社会模型，则会在对痛苦的刺激进行口述评分时，表现出相匹配的行为。然而，这些改变是他们的自发改变还是在痛苦中的真正改变，尚不清楚。
>
> 这项研究使用不同的测量方法以排除早期研究在方法上的局限性，通过测量非手掌部位皮肤的电位、手掌皮肤的电导系数和心率指数，测试实验参与者对电刺激的心理/生理反应，同时还使用知觉决策理论方法评估实验者对痛苦的表述。
>
> 非手掌皮肤电位和心率反应的几个指数显示出耐受人群的反应较小。忍受程度也与主观压力的减轻相关。实验结果与下述观点一致，即接触忍受模型后痛苦指数的改变代表的是痛苦经历的基本特征发生了变化，而不是有关信息受到主观抑制。

我们整理一下上面的内容，克雷格博士所做的基本上就是对人们施以电击，然后让他们标记痛苦级别。之后，在有能够“忍受”痛苦的人在场的时候，对实验参与者做同样的测试，但是改

变了电击强度。此时实验参与者似乎穿上了神奇的外衣，因为他们现在忍受痛苦的能力更强了。

该实验表明，表现出痛苦或者感觉痛苦的部分动机与周围人的表现相关。研究中的人们不是仅仅表现得好像痛苦减轻了，而是在能够“忍受”痛苦的人在场时，他们的皮肤和心率反应真实地反映出他们没有那么痛苦了。

一个古老的电视节目《真实视频秀》（*Candid Camera*）幽默地展示了社会认同的威力，视频详见www.social- engineer.org/framework/Influence_Tactics:_Consensus_or_Social_Proof。

视频展现了电梯中的实验对象如何在他们人的影响下面朝不同的方向站立，甚至在某一时刻会面向电梯内侧站立，因为其他人都这样。电梯实验中有4~5个参与者是我们特意安插进去的。每隔一段时间，这几个人会同时面向左、面向右或者面向后。几秒钟后，隐藏的摄像机捕捉到电梯里的其他人也开始模仿他们，面向同一方向、脱下帽子或者做其他动作。

社会认同可以说是社会工程中的一件致命武器。通过告诉对方其他人甚至是行为榜样都采取了某种行为或表现，可以刺激对方也这样做，这就是社会认同原则的作用。社会认同提供了一条决定应该如何表现的捷径，但同时也使得人们易被想要利用这种影响的其他人所操纵。

社会认同在以下两种情况下最具影响力。

- **不确定** 在人们不确定并且形势不明的情况下，他们更可能观察他人的行为，并认为这种行为是正确的。
- **相似性** 人们更倾向于跟随与自己类似的人的引导。

在这些情况下，社会工程人员可以运用社会认同工具。向目标明示或者暗示之前很多人采取过某一特定的行动，会提高成功的几率。

在一次社会工程活动中，我被机敏的保安人员拦住了，于是装成很疑惑的样子，说道：“昨天，吉姆检查我的证件后让我进去了，我刚才还以为你们有记录呢。”

保安听说吉姆同意我进去，就没再询问，让我进去了。社会认同不会总是这么容易，但是用起来功效会很强大。

本节提出的社会认同原则是当今所使用的最致命的影响战术。毫不夸张地说，这些战术为社会工程人员激发和诱导他人提供了强大的工具，使得社会工程人员可以控制他人的行为。

谨记，影响和说服的艺术是让他人以你希望的方式想要去做、行动、思考或相信的过程。为目标创造动机是一种强大的力量，可以说是社会工程的超级武器。前面提到的原则和方法可以让这件超级武器变成现实，但必须经过很多的工作才能产生相应的效果。

这样说意义何在？我经常发现在经过训练并熟练掌握某一技巧后，想要忘掉就很困难。社会认同似乎很有吸引力，但用于影响别人的时候应该特别小心，尤其是作为社会工程人员。要想让

这些技巧根深蒂固，就得用它们来帮助别人。例如，当你开始练习阅读微表情，甚至开始利用其操纵目标时，初始反应可能是觉得自己拥有了一项神秘的能力，几乎可以读心了。这就是需要小心的地方，你还需要练习技巧并不断精化，但是不要认为你已完全了解。

如果能说服他人戒烟，或者劝服他人开始锻炼身体，采取一种更健康的生活方式，就可以深入发掘这些技巧，去帮助他人。将这项技术运用到社会工程活动也就不是那么遥不可及的事情了。

很多技巧都需要真正地对人们感兴趣、关心他们并抱有同情心。如果这不是天性，就必须努力掌握这些技巧。我鼓励你花这个时间，因为这些技巧能让你成为一名优秀的社会工程人员。

设想你能改变自己的想法，让自己相信可以轻松地掌握这些技巧。再设想你能改变目标的想法，让他们体验到你想让他们体验的东西。设想你能随意改变交谈对象经历的事实，包括你自己的，这就是下一节的内容，它会让你感到震撼。

## 6.3　改动现实：框架

框架被定义为生活中的信息和经历，能够在人们必须作出决定的时候改变其反应方式。从非社会工程人员的角度来看，框架就是你和他人的个人经历，这些经历会影响你的意识，从而改变你作决定的方式。

食品店在碎牛肉的包装上贴的标签往往是“75%瘦肉”，而不是“25%肥肉”，这就是框架的一种应用方式。这两个标签意思完全相同（都有25%的肥肉），但前者听上去更有益于健康，所以对买家会更有吸引力，这也是商店选择使用前者作为标签的原因。

前面的例子很简单，但是能够帮助我们了解框架的作用。通过不同的方式呈现事实能够使通常被视为“不好”的事物看起来“很好”。

下面各小节列出了一些经常使用框架的领域，有助于你了解它的威力。

### 6.3.1　政治活动

框架在政治活动中的应用由来已久。单单是竞选和信息所使用的不同措辞就足以影响公众对这些信息的解读。

以认知语言学家乔治·拉考夫（George Lakoff）为例。在对政治活动中框架应用的一次有趣观察中，他陈述了人们对“通过法律实施反恐”和“通过战争反恐”这两种说法的不同看法。在“9·11恐怖袭击事件”发生时，科林·鲍威尔说这次袭击是一种犯罪。当公众要求采取更多的行动和更强硬的政策时，小布什总统宣布了“反恐战争”的发动。

另一个例子是美国的社会保障计划。这个名字的本义暗示这个计划值得依赖，能够为未来提供保障。

还有一个例子，就是“紧急援助”（bailout）和“经济刺激”这两个词的不同。紧急援助会遭遇很多反对的声音，因为这个词的字面意思是为正在下沉的船往外舀水。而经济刺激这个词给人的感觉是通过刺激经济来推动经济的发展。这两个计划的做法基本相同，但是不同的用词让后者更容易被人们接受。

朱迪思·巴特勒（Judith Butler）是加州大学伯克利分校的教授，也是备受好评的《战争的框架》（*Frames of War*）一书的作者。该书中特别描述了在西方文化中政治事件和战争发生时“框架”是如何使用的。下面是她对媒体描述“州暴力事件”的讨论。

> 这种描绘已经渗透到我们对人类生活的理解中，并导致对整个人群的不当对待和放弃。这些人被当做威胁而不是需要保护的、活生生的人。这些人被贴上了标签：迷失、监禁、失业、饥饿并且可以轻易解雇。在这种扭曲的逻辑中，为了保护“活人”的生命，放弃这部分人非常必要，牺牲他们的生命是合理的。

以上仅仅是政治活动中框架应用的几个例子。

### 6.3.2　在日常生活中使用框架

参考框架是一组看法、条件或假设，它们决定了人们如何接近、认知或理解某一事物。这个定义有助于我们理解框架的运用方式。

任何可以用来改变人们的认知或者人们作决定的方式的东西都可以称为框架。朋友告诉你上周她去了镇上，由于一些地方在修路，她比平常多走了16千米。你可能会为了避免迟到而选择一条更远的路，即使朋友是在一个多星期以前告诉你这一消息的。

我们的大脑天生不喜欢混乱或混沌。当混乱的事物出现时，大脑会尝试找出其中的规律。图6-4就是个有趣的例子。

在你目前的框架中，什么是背景？什么是前景？你可能会坚持在事物中寻找熟悉的图案。我们在面对云朵、天空或其他无生命的物体时都会这样做，人类倾向于在这些事物中发现面孔。

在观察图6-4时，你能改变思维框架，调换它的背景和前景吗？尝试调整你最初的认知，将前景和背景倒转。

人类大脑在混沌中寻找规律的另一个有趣的例子是前几年互联网上不断转发的一封邮件，其内容大致如下。[1]

① 原文中，每个单词中的字母顺序发生了改变，从而导致混乱。——译者注

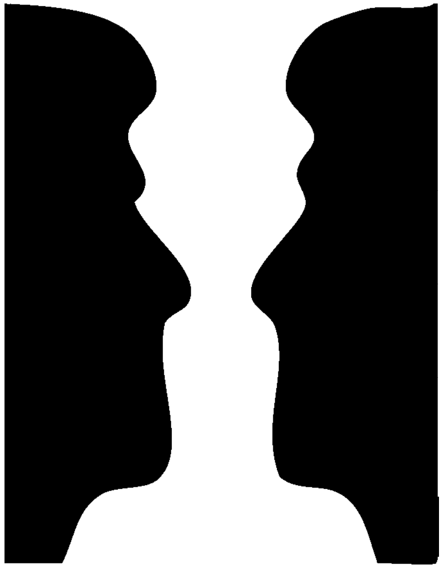


图6-4　你能通过改变现实框架看到不一样的东西吗

O lny srmat poelpe can raed tihs.

I cdnuolt blveiee taht I cluod aulaclty uesdnatnrd waht I was rdanieg. The phaonmneal pweor of the hmuan mnid, aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn't mttaer in waht oredr the ltteers in a wrod are, the olny iprmoatnt tihng is taht the frist and lsat ltteer be in the rghit pclae. The rset can be a taotl mses and you can sitll raed it wouthit a porbelm. Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe. Amzanig huh? yaeh and I awlyas tghuhot slpeling was ipmorantt! if you can raed tihs psas it on !!

翻译过来是：

只有聪明人才能看懂。

我不敢相信自己真的可以看懂这封邮件。这就是人类大脑不可思议的能力。根据剑桥大学的一项研究，单词中的字母顺序并不重要，唯一重要的是首末字母要正确。就算其他字母完全混乱，你也可以看懂。这是因为人类的大脑并不会阅读单词的每个字母，而是将它们作为一个整体来阅读。是不是很神奇？我曾经一直以为拼写很重要呢！如果你能看懂这封邮件，请转发！

我不知道这是否真的是剑桥大学的研究，但是有关这封邮件的很有趣的一点是，很多以英语为主要语言或者可以熟练阅读英文的人可能都可以毫不费力地阅读其中的文字，因为我们的大脑非常高效，能够从混乱中找出规律。

很多时候框架是难以察觉的。公司在市场营销中应用这一点，希望潜意识信息能够改变目标对其产品的认知。他们常常会使用微妙的框架方法植入信息。

例如，图6-5中显示的内容大家可能看到过很多次。




图6-5　你能识别出其中的框架吗

告诉你之后，你可能会彻底改变对FedEx标识的看法——这个标识中隐藏了一个箭头。在与标识设计者的访谈中，他说在标识中嵌入箭头是为了给人们植入一个有关FedEx服务的信息，用以显示FedEx公司的移动、速度和动态特性。

你找到了吗？请看图6-6，我将箭头用圆圈标注了出来。




图6-6　箭头表示永远移动的优质服务

FedEx不是唯一一家应用框架的公司。几十年来，各公司一直在他们的标识中嵌入框架信息，希望人们以其期许的方式记住和看待他们的公司。请看下面几个例子。

你能看出亚马逊公司标识中嵌入的框架信息吗（参见图6-7）？

amazon

图6-7　你能看到微笑着的满意的顾客吗

亚马逊的标识中有两个框架信息。一个是客户感到的快乐，以图片中的微笑表示。但是微笑同时也是一个箭头，这个箭头从A指向Z，表示亚马逊公司有你想要的所有东西。

另一个范例是立体脆（Tostitos）的标识。这是一个很有社交色彩的标识，请注意观察图6-8。




图6-8　这个标识会让你想和他人分享玉米片吗

图中央的两个T代表人们正在分享一块玉米片，中间是一碗洋葱番茄辣酱。2004年，立体脆公司召开了记者会，称："立体脆是一种'社会化小吃'。无论是聚会、观看盛大的比赛时，还是在简单的日常会面中，立体脆都有助于在亲友之间建立联系。这款新标识生动地体现了建立联系的想法。"

这些只是框架应用在市场营销中的一小部分例子。框架不一定要使用图形，重要的是目标感知的价值。目标对一件事物的认知会提高或降低它的价值。以高价位服饰店为例。当你走进去的时候，每件衣服都摆放得井然有序、整整齐齐，看起来非常完美。这时你的认知就是每件衣物的价值都与其所标注的高价相当。然而，如果你将其中的领带、衬衫或其他衣物从架子上拿下来，放到折扣商店中，将它们与其他2.5折商品放在一起，你会觉得这些物品的价值大打折扣。

营销大师利用这一现象影响公众对价值的认知。很多公司的框架战术都很成功，以至于人们会创造一种新型的词语来描述产品。

例如，每个人可能都会说："可以帮我将这个施乐①一下吗？"甚至在使用非施乐牌机器的时候也会这么说。施乐是一个品牌名称，不是机器类型。

最近的例子是，不管使用什么搜索引擎，人们都会说"你Google了吗？"，因为谷歌已经成为网络搜索的代名词。人们想用纸巾时，会说："请给我舒洁（Kleenex）。"

还有一些名称，大家可能并没有意识到它们其实是品牌名称（除非你生于它们出现的年代），其中包括：

- 阿司匹林（Aspirin）是德国拜耳公司的产品商标；
- 热水瓶（Thermos）是德国Thermos GmbH公司的产品名称；
- 邦迪（Band-Aid）是美国强生公司的商标；
- 飞盘（Frisbee）是美国Wham-O公司的商标。

① 施乐（Xerox）是最有名和最早的复印机品牌。——译者注

所有这些名字如今已经非常流行，人们在遇到任何类似产品时都会用它们来作为框架参考。我从不服用阿司匹林（通常服用另一品牌的药物），但是我会说“来两片阿司匹林”，而得到的总是我惯用的品牌，对此我很满意。

虽然存在大量与框架相关的信息，但是必须对这些信息进行概括和提炼，形成一些主要的原则，才能将它们运用于真实的社会工程中。前面对框架的概念及其在日常生活中的应用描述得很详细。在进入社会工程之前，先看一下框架联盟的不同类型。

### 6.3.3　框架联盟的 4 种类型

亚利桑那大学的戴维·斯诺（David Snow）和内布拉斯加大学的罗伯特·本福德（Robert Benford）合作写了一篇论文，标题为Clarifying the Relationship Between Framing and Ideology in the Study of Social Movements，详情参见http://www.social-engineer.org/resources/book/SNOW_BED.pdf。

斯诺和本福德认为，当个人的框架由于一致或互补而形成关联时，框架联盟就会出现，产生框架的共振，这是对群体进行框架转变的关键。斯诺和本福德随后列出了影响框架努力成果的4个条件。

- **框架努力成果的鲁棒性、完备性和彻底性**　斯诺和本福德找出了3个核心框架任务，对这些任务的关注程度将决定每个参与者投入的程度。

  3个步骤是：

  (1) 诊断框架的问题；

  (2) 分析并找出解决方案；

  (3) 如果成功了，号召行动。

  投入框架的努力越多，人们受框架影响从而采取行动的可能性就越大。
- **提议的框架和大众信仰系统之间的关系**　如果框架与人们的核心信仰或者信仰系统的价值没有任何联系，则人们会忽视该框架或提议的框架。

  如果一个人认为吃肉是虐待动物的行为，那么试图说服他去街上一家很有特色的西餐厅吃饭，肯定会失败的。框架必须与个人的核心信仰一致才能成功（除非你的目标是通过框架改变他的核心信仰），这对框架的应用非常重要。

  进行大规模框架改变的一个尝试是颇有争议的反对吸烟的广告，广告中志愿者将裹尸袋堆积在烟草产业大厦的大门口。裹尸袋代表每分钟、每小时或者每天有无数人因为吸烟而死亡。这次活动就是希望能改变那些支持吸烟的人的思维框架，让他们反思有多少人因吸烟而死亡。
- **框架与参与者现实情况的关联**　框架必须与目标本人相关。与目标经历的相关性必须可信且可验证。

  你不能通过市场营销框架鼓励那些每天吃不饱的人乘坐豪华邮轮，不管你多么擅于使用框架，结果只能是失败。如果要从框架发展到框架联盟，框架不能只是相关，还必须可证明，

哪怕这个证明只是存在于对象的思维中也没关系。

举个例子。2007年，广受欢迎的、可信度较高的新闻杂志《洞察力》（与《华盛顿时报》同属于一家公司）报道说，当时的总统候选人奥巴马曾就读于一所穆斯林学校，该校以教授激进和基本的伊斯兰教义闻名。这则新闻报道发布后，很多人立刻就相信了。为什么？因为这和他们的现实框架相吻合，这则消息似乎很可信，而且出自“可信的”媒体。

另一家声名卓著的新闻媒体CNN派出了调查人员，结果发现这个故事是伪造的，并将其发现报道了出来。

这是一个通过非常可信的渠道（新闻媒体）发布“事实”、改变人们对某一问题的思维框架的范例。那些想相信奥巴马是一个激进穆斯林的人很快相信了那个故事，消息飞快地传播开来。当研究揭示出故事是伪造的时候，很多人的思维模式又转变了回来。

- **反对的循环；对当前社会变迁的持续关注，以及框架在当前时代出现的时间点** 世界上正在发生的事情会影响社会框架。想想几年前，如果建议美国或者其他西方国家的公司进行全身X射线扫描，不啻于痴人说梦。

  提倡隐私保护的人会反对这一提议并会获胜，理由是他人会看到你的私处并可能保存这一照片以嘲笑你或者对你进行性骚扰。这一理由足以抹杀机器制造者在销售上所做的努力。

  然而，在美国发生“9・11恐怖袭击事件”后，恐怖主义活动兴起，于是这些机器被安装在了世界各地的机场，即便反对者大声抱怨，甚至拿出儿童色情法律这一强大武器都没有用。为什么？保障安全的社会框架已经发生了改变，所以这样一种新的做法就被公众接受了。

斯诺和本福德提议，当使用这4点构建适当的框架时，社会将通过框架联盟发生大规模的改变，比如社会运动所必需的那些改变。他们的研究重点在于整个社会，但是这些原则在处理小规模事件甚至是人与人之间的问题时也很有效。

前面讨论的主要是形成框架联盟的过程，事实上在这4个条件都满足的情况下可以产生4种不同类型的联盟。虽然上述很多方面针对的是框架在群体层面的应用，但是下面将讨论这4种框架联盟在个人层面的应用，展示如何将它们用在更小规模的事件上。这不仅适用于社会工程人员，也适用于想要和其他人在框架上达成一致的人。设想将你想进入建筑物的目标与保安想要阻止你的框架达成一致。将他的框架与你的伪装形成一致，就能确保成功。

必须记住一点，即框架从来都不是从头构建出来的。框架总是根据已有文化符号提出的，涉及个人信仰和经验的核心。懂得这一点将有助于你应用框架。

#### 1. 框架桥接

凯西・马什普查和调查研究中心（Cathie Marsh Centre for Census and Survey Research）将框架桥接定义为就某一主题而言思想上一致但结构上互不关联的两个或多个框架的联接。

桥接并不是诱使他人相信你的框架，而是在你深入了解了他们的框架后，发现了两者之间的联系，然后可以利用这一联系将目标带入你的框架。

以你想进入一个区域、大厦或者得到某些信息为例，你的框架是你想完成这一点，而你接近的那个人的框架未必就是要阻止你，他甚至不知道你想要做什么。如果让他认识到这一点，他就会真的这么做，这样你也就没有机会了。

通过了解目标的工作、角色和精神状态，可以掌握他的思维框架，这样就可能发现一种联系，使得他更加容易地进入你的框架。

你的伪装是什么？你要接近的那个人会如何对待你伪装的角色？优秀的社会工程人员只有理解这一点才能成功。“门卫”对待推销员和苏打水送货员的态度是不同的。理解目标的框架意味着知道他将如何对待你——不是如何对待社会工程人员，而是如何对待你伪装的角色。

一个针对个人的例子是考虑你想让他人如何看待你——酷、有能力、有才气或者自信。教授想要显得智力超群，经理想要表现控制力，运动员想要显得冷静和强壮，喜剧演员则希望观众认为他有趣。所有这些都是个人框架，而且希望他人的框架思维能够一致。

以喜剧演员为例，如果碰到一个质疑者，这个人认为他不酷、无趣、不聪明、不自信，怎么办？因为质疑者的认识框架，他们会愤怒、不高兴、不安还是不在乎？如果这个喜剧演员坚持他的框架，他会转换周围人的认识，但是只有当他深入探索并了解一些人的框架来源后，他才能最终在两种框架之间建立桥接联盟。能够应对质疑者的喜剧演员可以先将他对自己框架的恐惧放在一边，对质疑者加以利用。

框架桥接联盟技术可以成为社会工程人员最有力的工具之一，但是需要一些准备工作以确保正确运用。

社会工程人员可以利用这一特殊形式的框架联盟，通过适当的伪装帮助目标将他们看到的和他们应该相信的内容联系在一起。请再次回忆伪装成技术支持人员尝试进入大厦的例子，你的着装、工具和言谈必须和目标认识的技术支持人员匹配。如果做到了，则桥接成功创建，联盟产生。

### 2. 框架放大

根据戴维·斯诺的定义，框架放大是指“对一个与某议题、问题或者一组事件有关的解释性框架进行阐述及激励”。换句话说，你要扩大或者把焦点放在目标的价值观或信仰上。通过将焦点集中在目标关注的价值观上，就能找到连接两者思维框架的区域，或者至少让目标认为存在一个联盟。

这种类型的联盟是4种联盟中最基本的，因为它主要是一种防御性方法。它通常会涉及强调某一事件比其他事件更加重要，从而使得这个事件能够轻松地与其他事件联系起来。

如果仔细研究前面所述的全身X光扫描器的例子，就能发现其中的框架放大方法。扫描器现在是作为阻止恐怖分子的设备进行销售的，是最近的恐怖主义活动使此类产品有了市场，所以在我们的框架中需要此类设备来满足需求。然而研究显示，市场上此类设备早已存在，只是在9·11

和其他袭击事件发生之前，人们一直拒绝使用。

利用“9·11恐怖袭击事件”以及人们因类似袭击事件而产生的害怕乘飞机的心理，扫描器公司将他们的思维框架与很多人的恐惧心理框架联系起来，从而使人们支持其在全球各机场部署这些设备。

框架放大的另一个用途就是它能够成功让现有的框架产生混乱，使得具有特定信仰的人远离他们的信仰。例如，很多人重视隐私并且认为自己有选择扫描方式的自由，但是他们被X光扫描设备的生产厂家所影响从而改变了框架，因为生产厂家着重强调了其他扫描方法不完善或者不安全，而且为了证明这一观点，还拿出了类似“内衣炸弹”的故事。这些战术放大了他们的框架，说明新的X光扫描设备更好、更安全，利用了人们普遍相信其他方法不安全的心理。

社会工程人员可以通过不同的方法利用这种联盟战术。例如，社会工程人员想要说服保安让他进入现场的垃圾箱区域。伪装成废品处理合约商的工作人员就是一个好方法。这一方法本身就可能成功，如果再说明其中一个垃圾箱出了问题需要处理，则会更容易达到目的，因为它是公司的一个安全隐患。放大这一思维框架可以让你和保安达成一致，让他相信最好的方法就是让你到现场进行检查。

### 3. 框架扩展

“框架扩展是一种变动的成果，通过将提议的框架的边界扩展到一群人的观点、兴趣，特别是情绪，将参与者引入其中。”换句话说，通过扩展框架的边界，将目标的其他主题或兴趣引入其中，就能与他们达成联盟或一致。

例如，那些支持环境保护或者“绿色”主张的人可能会将他们的框架扩展到反核运动，其主要原因就是他们担心环境风险。

不过，使用框架扩展战术可能会削弱人们对原有框架的支持，导致其在一定程度上丧失吸引力。如果在给定框架中包括太多的扩展，就可能出现这种后果，即逐渐地稀释并最终使人们对主框架失去兴趣。

甚至从个人层面来讲，简单的也是最好的。在使用这种框架结盟战术时，尽量使它简单、易于遵循。不要让连接的网络太过错综复杂，以致最终让目标失去兴趣。

社会工程人员可以通过第3章讨论的诱导技术使用这一框架联盟方法。当社会工程人员接近目标时，可以通过聚会中的闲聊，在不经意间套取目标或其公司的信息，也可以伪装成记者。这会赋予社会工程人员询问信息的“权力”，而这种信息通常很难获取。

### 4. 框架转换

“当提议的框架很难引起共鸣，而且有时与传统的生活方式、礼制以及现有的解释框架背道

而驰的时候，就需要进行框架转换。”换句话说，社会工程人员通过提出新的论点说明为什么他们的框架更好，意图将目标原有的框架思维和信念转换成社会工程人员希望的样子。

在框架转换发生时，需要新的价值观和理念来确保人们参与其中，并得到他们的支持。20世纪70年代，当保守运动的思维框架重新形成或者说转换成一种更加激进的环境保护运动时，就是一种大规模社会框架的转换。

在个人层面，通过宗教信仰的改变，框架转换每天都会发生。此时，个人框架或者整个信仰系统都会发生改变，与新的信仰和新的思维框架形成一致。

转换一个人的框架并不容易，这也是实践中一种最复杂的战术，因为它需要：

- **时间**　改变一个人的整个信仰结构不是一蹴而就的事，它需要用到其他联盟技巧，并且需要花费很长时间才能成功。
- **精力**　了解目标的框架并确定你希望他接受的新框架只是万里长征的第一步。他拒绝的理由和思维障碍是什么？找出这些实非易事。
- **教育**　知识就是力量。必须帮助目标理解你想要他“转换”到的新框架。
- **逻辑**　教育必须合乎逻辑而不全是以情感人。目标必须能够论证并认为其即将采取的行动合理。这只能通过逻辑达到。
- **深厚的感情纽带**　知识是行动的前提。逻辑能够说服他采取行动是对的，但是感情会促成行动的发生。如果你投入了感情，目标会感知它的存在。确保你表达的感情和感受与伪装的角色相匹配。如果你的伪装是指导顾问，而你却表现得像个啦啦队长，那么目标是不会与你结成结盟的。

如果能够让他人的框架与你的框架结盟并且形成一致，就能激励目标做你想要的事情。虽然上述4种结盟方式都很强大，但是只有成功掌握框架转换的社会工程人员才能具有无穷的力量。

请继续了解社会工程人员如何应用这些框架战术。

### 6.3.4　社会工程人员如何利用框架战术

本节将讨论社会工程人员使用框架战术的多种方法。其中一些方法很强大，如果能够熟练掌握并且准确地利用，你将成为一位影响大师。

要想在社会工程中真正使用框架战术，必须理解其中的4条规则。这4条规则将有助于你清晰地理解框架是如何工作的，以及怎样在社会工程过程中使用它。

请记住什么是框架。框架就是我们思维的概念性结构。这是一个很重要的信息，因为你的目标就是创建一个新的框架，或者与他人形成框架联盟，或者将目标带入你的框架。

这3个目标中的任何一个都需要你掌握下面4条规则，这样才能在社会工程过程中应用框架战术。

**规则1：你说的每件事都会唤起一个框架**

人们的思维过程就是描绘事物的过程。这一事实是不可能更改的，但是你可以利用它实现自己的目标。

如果我开始和你讨论你的老板，你的大脑就会对其进行描绘。如果我说他在外面打手机并且很愤怒，你的大脑就会开始描绘他愤怒的面容、肢体语言和所说的话。你无法控制这些，这一思维框架会激起你的情绪和反应。

用话语进行描绘是使用框架的一种强大的方法。通过精心选择用词，可以让目标的大脑描绘你想让他描绘的事物，将其移动到你设定的框架中。

你听过某个你认为特别擅长讲故事的人讲的故事吗？为什么？他擅长的原因何在？他能够描绘心理图景，让你在头脑中看见事物，从而激起你的兴趣并融入其中。这一技巧对社会工程人员来说非常重要。这并不是说任何时候都要像讲故事一样说话，但是你要牢记自己准备的词句，因为这些话具有在目标的头脑中勾画情景的强大作用。

这里有个简单的例子：我告诉你我昨晚吃的是意大利面。如果你不是美食家也不是意大利人，或者上次吃意大利面的经历不是那么愉快，那么你的思维框架就不会很强大，也就会无动于衷。

如果我告诉你昨晚我妻子用她自己种的番茄和罗勒做了美味的番茄酱，其中还加入了新鲜的大蒜和牛至，并用红酒调味，之后她将番茄酱浇在精心烹制的面条上，并配以自己做的蒜香面包。这种描述会引起你怎样的反应呢？

不管你是否喜欢意大利面，大脑中都会出现一碟美味的食物。这就是在面对目标时精心选择词句的结果。这种方法描述性更强、更有画面感，也更有冲击力。然而社会工程人员也要小心，你的描述不能太过戏剧化。你的目的是通过话语描绘出一幅画面，而不是让目标关注你或者你的表达。

**规则2：框架中定义的词句会唤起思维框架**

不必使用最确切的字词来为他人描述你所设想的框架。例如，在阅读下面的句子时，你想到了什么？

“我看到昆虫在网中挣扎想要逃离，但是没能成功。一会儿工夫，它就被包裹在茧中，成了别人的晚餐。”

请注意，我并没有提到蜘蛛，但是你已经想到它了。可见我可以在不提及蜘蛛的情况下让你想到它。这一有关影响和框架的强大规则，使得社会工程人员可以通过间接表达来控制对象的思维。

旨在帮助人们提高表达能力的国际性组织Toastmasters，教导其会员通过语言调动听众的情

绪来打动他们。如果你讲的故事能够让目标描绘出你设想的框架，并让他们投入感情，你就能更好地主导对话。

同样，使用这种框架方法需要事先计划。这一规则的强大之处在于，目标的大脑在处理你提供的信息并生成你描绘的心理图景时，你可以植入想法。与我直接描绘美味意大利面不同，这一规则允许目标自由描绘。

在前面意大利面晚餐故事的结尾，我可以说："之后我妻子将番茄酱浇在了精心烹制的面条上。什么样的面条？我不会告诉你，你必须自己想象。"当你的大脑开始描绘的时候，我会说："当我用叉子卷面的时候，酱很浓稠，附着在每一根面条上。"

这描绘的正是意大利面。还有其他面条需要用叉子卷动吗？（我知道有，但你已了解了重点。）

**规则3：否定框架**

如果我告诉你不要想象蜘蛛在网中的情景，你会首先在大脑中想象蜘蛛，然后告诉自己不要去想它。

这种否定框架战术很强大。告诉目标要小心、当心或者提防某事，会自动将其引入你想要的框架。这种战术常被专业的社会工程人员使用。在我与一群社会工程人员交流的时候，每个人都同意这种战术很有用。

在一次审计中，我故意丢下几个带有恶意代码的U盘，希望公司里的某个人会不假思索地运行它们。我走近一个已获得其信任的员工，说道："约翰，我听说发出的备忘中提到要注意一些丢落的U盘，他们现在正找呢。"

事情就是这样发生的，你是管理员，丢下几个装有恶意文件的U盘，现在告诉别人要找到它们，这在本质上等于植入了让他们执行你命令的种子。这种表达方式消除了他们在找到带有恶意文件的U盘时的担心，让他们在找到的时候会插入电脑查看这个U盘到底是谁的。

**规则4：让目标思考框架会强化框架**

每次大脑在关注或考虑某事的时候，该事件都会得到强化。你让目标对你想让其接受的框架考虑或者描绘得越多，框架也就越容易得到强化，目标也就越容易陷入其中。

我们来回顾一下第2章所述的通信模型，分析一下社会工程人员发出的消息是怎样对目标产生影响的。

有一次我去印度旅行。我已经忘记新闻中提到的确切事件了，但是我记得当时乔治·W.布什总统让欧洲人民很生气。我浏览新闻站点，看到欧洲国家的人们把貌似布什的玩偶悬挂在街上，然后用美国国旗将玩偶包裹起来并焚烧殆尽。

我被当时的情景震惊了，当晚和妻子通话时说："哇噢，有关欧洲发生事件的这些新闻真是

疯狂，是不是？”

她没有听到任何有关这方面的事情。为什么？新闻媒体和新闻站点主宰并操纵了人们的思维框架。

社会工程人员可以通过学习媒体的这种技巧来提高自己的能力。通过省略、遗漏故事的细节，或者干脆不提这件事，媒体让人们得出了似乎是自己的结论，事实上这一结论来自媒体。

社会工程人员也可以这样做。通过省略某些细节，仅“透露”想要透露的细节，可以创建出他们想要目标思考或感觉的框架。

媒体使用的另一个战术是**贴标签**。当想要将某事定义为正面的时候，他们会说：“强大的防卫……”或者“健康的经济发展”。这些语句描绘出的心理图景是稳定和健康，会帮助人们得出正面的结论。同样的规则也适用于否定的框架。类似“伊斯兰恐怖分子”或者“阴谋论”这样的标签描绘出的就是负面的图景。

可以利用这一技巧，通过描述性词句为事物打上标签，将目标带入你设定的框架。有一次，我昂首阔步地往前走，突然被门卫挡了下来，于是我惊讶地看着门卫，歉意地说：“哦，昨天那个乐于助人的保安汤姆检查了我的证件后让我进去了，所以我以为有记录呢。”

将前面一个门卫说成“乐于助人”让现在的门卫自动进入了我设定的框架。如果他也想得到这样一个美好的标签，也应该像汤姆一样“乐于助人”才行。

框架之所以有效，是因为它扭曲了事实但又不至于太过虚假，所以仍然可信。社会工程人员可以创建想要的图景，但不能完全脱离事实。

我读过一个白皮书，标题为Status Quo Framing Increases Support for Torture，作者是克里斯蒂安·克兰多尔（Christian Crandall）、斯科特·艾德尔曼（Scott Eidelman）、琳达·斯基塔卡（Linda Skitka）和斯科特·摩根（Scott Morgan），他们是来自不同大学的研究人员。白皮书中提供了一个非常有趣的数据集，让我对这一课题兴趣盎然。在美国，似乎大多数人都反对在战争中使用拷打的方法获取情报信息。这一研究的目的就是要了解，研究人员是否能够通过不同的框架表达，让一部分人同意拷打并非不可接受的方法。

他们的采集样本有486个人，这些人要阅读两段文字。

第一段内容如下。

> 新闻中说，美国军队在中东地区审讯嫌疑人时采用了压力审讯的方法。根据一些报道，这种压力审讯是一种新的审讯形式，首次在美国军队中广泛使用。美国军方使用了多种方式，包括将嫌疑人绑在木板上浸在水中、将嫌疑人的脸按在睡袋中、用绳子将嫌疑人绑成痛苦的姿势长时间悬吊。此外还会让嫌疑人独处，并且连续多日不眠不休。

这段话让人们认为这些是美国政府为了获取信息而采用的新方法。

第二段内容如下。

> 新闻中说，美国军队在中东地区审讯嫌疑人时采用了压力审讯的方法。根据一些报道，这种压力审讯并不是一种新的审讯形式，已被美国军队使用了40多年。美国军方使用了多种方式，包括将嫌疑人绑在木板上浸在水中、将嫌疑人的脸按在睡袋中、用绳子将嫌疑人绑成痛苦的姿势长时间悬吊。此外还会让嫌疑人独处，并且连续多日不眠不休。

这一段与上一段的内容基本一样，只是第2句话被替换为“根据一些报道，这种压力审讯并不是一种新的审讯形式，已被美国军队使用了40多年。”

这两段话的思维框架分别是“这些是全新的方法”和“这些方法已使用了几十年，经过了反复的检验”。在更改了框架后，结果如何？

白皮书中描述了研究者的测量方法。7个选项形成了一组相互依属的基础变量。这些选项对应7个不同的“按钮”，依次为：强烈反对、基本不同意、有些不同意、不确定、有点同意、基本同意和非常赞同。对各项进行反向打分，得分越高表示越赞同。

结果呢？“描述现状的操纵方法对拷打的最后评价产生了影响——当表述为‘长期使用’而不是‘新方法’的时候，拷打的评分*更加正面*。让拷打看似一种常用的审讯方式，这提高了参与者对该方法的支持度，也增强了其合理性。”

通过改变框架中的一小部分，研究者和大量参与者建立了联盟，让他们同意（大体上）拷打是一种可以接受的方式。

文章继续评论道：“它们可以应用于很多领域，可以影响人们的判断、决策、审美观以及政治倾向。”而结论是：“适当改变呈现、设定道德选择和价值困境的方式，会对人们的政治选择和政策产生意义深远的影响。”

这一实验证明了框架战术的强大，因为它甚至能改变人们多年秉持的核心观念、判断和决定。对社会工程人员来说，大部分时候不需要设定这么高的目标，并不需要尝试改变人们的观念，只需要让人们采取一些细想时会觉得不妥的行动。

采用这4个框架规则并进行细致的计划，能够让框架成为摧毁性武器，不过这也是恶意社会工程人员每天都在使用这一战术的原因。在美国，特别是“西方文化”中，人们接受的教育就是要接受框架的影响、接受被灌输要思考什么以及怎样思考。

如果我15年前告诉你，几乎每个电视节目都是看真人生活秀，你一定会笑我。为什么？因为观看那样的节目似乎无聊又愚蠢。然而在2006年，《洛杉矶时报》声称现实类电视节目的数目提高了28%（详见http://articles.latimes.com/2010/mar/31/business/la-fi-ct-onlocation31-2010mar31），

而且在此之后没有明显的回落，因为观看这类节目显示了时尚与新潮，因为我们被告知这种节目好看且有趣，而且所有人都在看。这类节目作为一个例子，说明了一件几年前大部分人认为愚蠢的事情，现在可以变成适合做的事。

框架绝对是一种艺术形式，在与沟通和影响等科学相结合之后，就会变成熟练社会工程人员手中的强大武器，通过以某种形式传达信息后，社会工程人员就能够“轻易”地与目标形成联盟，促使目标在不会感到内疚的情况下采取行动，改变目标对现实的感知。

框架和影响是社会工程的重要组成部分，但后者经常与社会工程的“黑暗角落”联系起来。本书文前提到了这些角落，下一节内容会改变你对“影响”的看法。

## 6.4 操纵：控制你的目标

对很多人来说，操纵是一个很黑暗的话题，因为在通常的描述方式中，它会让人产生一种畏惧感。

看一下在互联网上找到的几个关于操纵的定义，就能理解上面一段话的含义。

- “运用精明、迂回的影响，尤其是为了自身的利益”
- “精明、迂回地影响或控制”
- “巧妙地控制或者影响（他人或自己），通常是为了个人的利益”

通过上面的定义，我们能够明白为什么很多社会工程人员偏爱这一主题。通过自身的技巧控制或影响他人，达到自己的目的，你能想象这有多大的吸引力吗？

从阴暗的洗脑手法到销售员使用的隐晦暗示，操纵是每个社会工程人员都应该学习并精通的技巧。操纵的目的就是要战胜目标的批判性思维和自由意志。当目标基于熟悉的流程无法作出决定的时候，操纵的人可以给他灌输想法、价值观、态度或者道理。

操纵有6种使用方法，适用于洗脑及那些不那么阴险的方式。在深入探讨之前我们先简要熟悉一下各个方法。

- **提高目标的暗示感受性** 在最极端的情况下，睡眠或者食物匮乏会提高目标的暗示感受性。在缓和的方式下，时间紧迫的隐晦暗示会让目标更容易受影响。
- **获取目标环境的控制权** 这一技术包括的范围很广，从基本的方法，如控制目标能够访问的信息类型和数量，到某些微妙的方法，如获取目标的社交网站的访问权。在社会工程的背景下，如果能够访问目标的社交媒体，就可以查看目标的交流信息，并对目标收到的信息进行控制。
- **制造怀疑** 动摇并深挖目标的信仰系统，这对控制目标采取你想要的行动会大有裨益。

从社会工程的角度来看，这种方式必须巧妙。不能一上来就贬低目标，相反，可以质疑他们执行的制度、工作或者信念，逐步影响目标作出理性决策的能力。

- **制造无能为力的感觉** 这是应用于战时审问的一种恶意方法，会令目标对自己的信念逐步丧失信心。社会工程人员可以利用这一技术，通过显示你从某一权威人物处获得的“事实”，对目标釜底抽薪，让他们感到无能为力。
- **让目标产生强烈的情绪反应** 强烈的情绪反应包括怀疑、罪恶感及耻辱等。如果情绪足够强烈，就会让目标改变整个信念系统。社会工程人员必须小心翼翼，不能制造破坏性的负面情绪，但是制造害怕失去或害怕受到惩罚等情绪反应，对最终的社会工程目标达成会起到促进作用。
- **严重威胁** 对生理痛苦或者其他可怕情形的畏惧能够让目标在压力之下崩溃。同样，除非是伪装成商业间谍，大多数社会工程人员是不会使用这一方法的。在常规的社会工程活动中，这种方法通常利用权威制造强烈的恐惧感或者有潜在损失的感觉。

不过大部分时候，操纵并不是这样极端。设想一个最简单的场景，你在一个拥挤的房间中，有人叫你的名字，你会有什么反应？你通常会转身问：“谁啊？”此时你就被操纵了，只不过这不一定是带有恶意的操纵。

在心理层面，被操纵的情况更加复杂。请注意前面的反应发生时的具体情况：大脑听到你的名字，你自动形成一个应答（“谁啊？”）。应答和发出声音之间的连接非常短。即使你不出声响应或者那人叫的并不是你，大脑在接收到问题时也会形成应答。

近距离听到两个人交谈并且无意中听到一个问题，你的大脑就会形成一个应答。应答可能是头脑中的一幅画面或者一个声音。如果目标无意中听到两个人在谈论类似他头脑中的某个人，他的大脑中就会出现一个画面。如果你听到两个人在说小鸡过马路的笑话，大脑中就会出现小鸡、马路或者整个场景。

这种类型的操纵对你来说只是个开始，另一种操纵技术则需要条件反射。

通过不断地适应，人们会将特定的声音、行为与感觉和情绪相关联，形成条件反射。如果每次提到积极的事物时目标都会听到钢笔的咔嗒声，那么一段时间后，目标就会将这种声音与积极的感觉相联系。

一个最经典的条件反射的例子出自伊凡・巴甫洛夫之手，我们常称之为“巴甫洛夫的狗”，第5章曾讨论过这个例子。问题是我们能否将这种训练施加于人。虽然让目标流口水并不在大多数社会工程人员的优选策略列表中（这是一个笑话），但是能够训练目标在接收到特定输入时，按照你想要的方式响应吗？

要找出答案，请继续阅读下面的小节，其中提供了几个商业和市场营销领域的操纵实例，为我们讨论和分析如何进行个人层面的操纵奠定了基础。

## 6.4.1 召回还是不召回

2010年5月，《华盛顿邮报》报导了一个有趣的故事，详见www.washingtonpost.com/wp-dyn/content/article/2010/05/27/AR2010052705484.html。儿童用羟苯基乙酰胺（Tylenol）、布洛芬制剂（Motrin）、可他敏（Benadryl）和仙特明（Zyrtec）的制造商，在液态非处方药中发现一批布洛芬制剂存在缺陷，但是又不想花费一大笔钱来召回，那么公司是如何回应的呢？

他们使用了操纵战术。公司雇用了许多合同工，让他们到每家药店买下所有布洛芬制剂，然后销毁。不幸的是，由于某合同工的疏忽，写有该计划的一份文件失落在了其中一家药店，随后这件事就被报告给了美国联邦药品管理局（FDA）。

根据备忘录，FDA确实让该公司分4次召回所有问题药品，其中的一次召回就达到了1.36亿瓶。只是已经太晚了，因为报告称已经有775名儿童和婴儿由于服用这批药品产生了不良反应，最终有37例病亡。报告中并没有说是问题布洛芬制剂还是对布洛芬制剂的反应导致了死亡。那不是我们讨论的重点。

这是一个非常阴险的操纵实例，至少是尝试操纵。为了保护公司形象，他们竟然放弃了正确的流程且不顾全世界儿童的生命安全。他们尝试对系统进行操纵，结果有人因此而丧命。遗失在药店的文件内容主要是讨论合同工怎样奉命买回产品，只字未提“召回”。

事情败露后，他们执行了很多有趣的操纵战术。他们歪曲事实说之所以这样做，是因为专家认为该制剂对儿童来说并不存在很大的风险。

在此之后，他们正式道歉，并且解雇了6名高管，然后开始进行真正的操纵了。在被质询时，公司说他们不是在尝试人们所说的“隐秘地召回”，而是要检验所谓的有害批次药品，所以让合同工将药品买回来测试。如果发现确实有问题，公司会采取正确的流程。公司尝试使用操纵战术中的转移方法，将人们的注意力从他们的事实行为上转移，以使情况看起来没那么糟糕。他们还使用了掩饰方法，操纵那些不认可他们行为的人，声明公司正在尝试测试以确定是否需要召回。

这种类型的操纵值得讨论，因为转移策略也适用于个人层面的操纵。如果你去了不该去的地方，并且被抓住了，那么编一个可信的故事有助于你操纵目标，让你顺利过关。将目标的注意力从当前问题上转移，会为你赢得时间，改变目标的关注焦点。例如，如果你被保安人员逮个正着，不要紧张，冷静地看着他说：“你知道我在这里做什么吗？你听说一些包含非常重要数据的U盘丢失了吗？我们要在明天上班之前找到，这非常重要。你要检查盥洗室吗？”

很多人可能从没有听说过布洛芬制剂召回事件，这也显示了公司在操纵媒体和司法系统方面做得很好，所以没有成为人们关注的焦点。不管怎样，这个故事展示了转移和掩饰方法在操纵战术中的使用。

## 6.4.2　焦虑的最终治愈

1998年，世界上最大的制药公司之一史克必成（SmithKline Beecham）发起了一波广告宣传，意在向大众传播“社交焦虑症”的概念。他们发布了50个新闻故事及调查，提出 “你有社交焦虑症吗？”之类的问题。这些测试和调查都旨在告知人们什么是社交焦虑症以及如何判断自身是否患有该病症。

之后，他们又更改了医学杂志中的宣传广告文案，由“帕罗西汀（Paxil）意味着……从抑郁症、恐慌症和强迫症中恢复平静”改成了“让他们知道自己能……第一种也是唯一一种获得认可的社交焦虑症治疗方法”。这一转变花费了公司大约100万美元。

1999年，他们又发起了新一轮耗资3000万美元的宣传，在平面媒体和电视上宣布史克必成找到了治愈社交焦虑症的良药，它的名字就是帕罗西汀。公司买下了当时一些热门电视节目中的固定节目档，使用调查和测试中获得的数据，吹嘘统计数据表明有1000万美国人患有社交焦虑症，现在他们有希望了。

到2000年，帕罗西汀在这一快速增长的市场中获得了一半的份额。公司斩获“2000年美国新型抗抑郁药（选择性5羟色胺再吸收抑制剂）零售处方市场的第一名”。2001年，FDA批准该公司销售帕罗西汀，用于治疗一般性焦虑症和创伤后应激障碍。

“9・11恐怖袭击事件”导致所有抗抑郁和抗焦虑药物处方量的巨幅增长。在那段时间里，帕罗西汀的广告定位是能够解决恐怖袭击后人们普遍具有的恐惧感和无助感。

我并不是说这类药物完全没有作用，也不是说公司的动机险恶，但是我发现这个案例中对市场的操纵特别有趣，开始时是教育和宣传，最终是销量的大幅增长，在此过程中还创造出了新型的失调。

这种问题构造的操纵方法常用于市场宣传，但是也应用于政治甚至个人层面，首先提出一个可怕的问题，然后提供“事实”作为证据，证明你所说的是真实的。在一期《骗术真相》节目中，保罗・威尔森设置了一个场景，在骗局中他让一位明星从商店里偷CD。商店雇员扣押了明星，等待警察的到来。之后保罗走了进来，说自己就是警察，还将他的钱包在对方眼前晃了一下，钱包中只有他小孩的照片，然后他“逮”走了明星，并且将CD和收银机中的现金一起作为证据带走了，没有人提出质疑。这个故事非常适用于说明这类问题构造的操纵方法。保罗有一个问题（小偷明星），然后将自己装扮成问题的解决方案（警察）。不管场景如何，在提出你的要求之前，要构造一个问题，以方便你这个好人出场，而那个问题会让你想操纵的人接受你的要求。

### 6.4.3　你不能让我买那个

卡马特[①]。我很想在这一节只写这一个词，但感觉还是得多解释一下。卡马特提出了一种思路，称为产品陈列示意图或者货架图，通过这个图告诉零售商怎样基于产品的颜色、尺寸和其他标准来展示其产品，以刺激顾客购买和消费的欲望。

货架图旨在优化视觉效果和商品摆放。

这些图的使用就是一种形式的操纵，因为研究者仔细分析了人们逛商店、思考和购买的方式。通过对这些方面的理解，他们设计出了控制视觉输入的机制，从而刺激购物者的购买欲望。

软件以及整个公司都致力于计划和执行这些货架图，以期达到让客户尽可能多购物的效果。

他们使用了3种操纵购物者的布局方式。

- **水平放置商品**　要提高顾客对特定商品的注意力，可以将此种商品一个挨一个地水平放置。一些零售商发现，一种商品的最小放置区间在15~30厘米，这样才能有效吸引顾客的注意力（参见图6-9）。



图6-9　水平放置同样或类似的物品以吸引顾客的注意力

- **垂直放置商品**　垂直放置商品是另一种布局方式。这种方式下，每种商品占据不止一层货架的位置，以占据15~30厘米的放置空间（参见图6-10）。

① 财富500强公司之一，总部位于美国，主要从事零售业务。——译者注




图6-10　同样的商品放置在多行货架中

- **块放置**　具有一定共性的商品放置在一个块（品牌）中。可以并排放置、上下堆叠、中心环绕，也可以使用磁力挂钩等各种方式（参见图6-11）。



图6-11　类似商品或品牌的块放置方式

货架图不是操纵购物者的唯一方法。还有一个测试，即在商场内循环播放特别设计的音乐。结果是在播放音乐的情况下，购物者在大卖场内的购物时间平均会增加18%。

杰-查尔斯·沙巴特（Jean-Charles Chebat）和理查德·米琼（Richard Michon）在《商业研究期刊》上发表了一篇有关加拿大大型购物中心的研究论文（详见www.ryerson.ca/~rmichon/Publications/Ambient%20odors.pdf）。研究者在空气中喷洒特别设计的香味，意图促发购物者的快乐情绪、刺激购物。结果是在一周的研究时间里，平均每个购物者会多买50美元的东西。

去大型购物中心和水果店的体验肯定不一样。不过，从这些方法和实验中我们能学到很多。了解大脑对事物的分类方法，有助于你组织自己的"货架"，以便操纵目标的感觉、情绪和思维。

再来说一下色彩，它们是操纵目标情绪的一种主要方式。放置商品的原则同样适用于色彩。你的衣物或者用品的色彩能够对目标产生影响。很多研究的主题是色彩及其效果。下面列出了一些通过色彩影响人们思维或情绪的方法。

- **白色** 白色经常和纯洁、明亮以及干净联系在一起。它给人的感觉是安全、中立、善良和忠诚。这也是为什么白色常用于婚礼服装，或者用于表示投降。
- **黑色** 黑色通常象征权力、高雅、神秘和力量，常用来表示权威、深度和稳定。黑色给人的感觉是平静和宁静。通过对比，它也可以强化其他色彩。
- **红色** 红色和兴奋与喜悦相关联，是充满喜庆、行动和能量的色彩。它象征健康、速度、激情、欲望和爱。红色能够刺激情绪，使得心跳、呼吸加快，血压升高。

  红色能够引发强烈的情绪，在使用时需要注意。它能够表示力量和冲动，也能够代表武力、威胁和征服，甚至是暴力和复仇。请小心使用。
- **橙色** 橙色给人以温暖、热情、吸引、决心、力量和忍耐的感觉。它能给人以鼓舞和活力，甚至能刺激人的食欲。

  橙色是另一个需要审慎使用的色彩。虽然使用橙色有很多好处，例如让对方觉得温暖，增强你和产品的吸引力，但是用得太多或者组合不好的话会产生不安全、无知和迟缓的感觉。
- **金色** 金色常与明亮、智慧、财富和威望联系在一起。
- **黄色** 黄色与能量、乐观、喜悦、高兴、忠诚和精神饱满相关联。它能让对方觉得成为焦点和受重视。

  黄色也能影响一个人的记忆（这就是贴纸多为黄色的原因）。少量应用会激发正面的情绪，但是用得太多会让目标注意力不集中或者感觉吹毛求疵。
- **绿色** 绿色常与大自然、和谐、生命、丰饶、雄心、保护与和平相联系。它能够让人觉得平静、安全。

  绿色是另一种强有力的色彩，但是如果使用不当或者使用过多的话，也能给人以贪婪、内疚、妒忌和混乱的感觉。
- **蓝色** 蓝色是天空和海洋的色彩。它与智慧、直觉、真理、宁静、健康、力量和知识相联系。它具有让人镇定和冷静的力量，会让人的新陈代谢减慢。

  蓝色是眼睛最容易适应的颜色。它有很多正面的效果，但是运用时得注意，不要让目标觉得寒冷或者沮丧。

- **紫色**　紫色与皇家、高贵、奢侈、创意和神秘相关联。
- **棕色**　棕色与地球、可靠、易接近、惯例和秩序相关。它能给人以牢固或相关的感觉，或者一种秩序感。

你要如何使用这些信息呢？这里并不是说穿一身蓝色服装就能让对方感觉平静并将密码告诉你。不过你能利用这些信息筹划攻击方法，确保获得最佳的成功机会，计划中也要包括你的外表和着装。

社会工程人员必须仔细分析即将拜访的目标，确保着装的色彩能够增强操纵目标的能力，而不是让目标反感。例如，了解到绿色可能引发贪婪或野心的感觉，社会工程人员在与慈善机构会面时就不要穿绿色的衣服，因为它可能产生与慈善的使命相违背的感觉或情绪。另一方面，如果穿着蓝色套装拜访律师，就能起到让人冷静的效果，让律师敞开心扉。小心筹划并合理应用这些战术，能够确保社会工程审计的成功。

### 6.4.4　令目标积极地响应

条件反射用在日常交谈、市场宣传、恶意操纵等各个方面。就像巴甫洛夫的狗一样，通过训练，人们会对特定事物产生条件发射。人类的天性通常被用于操纵大部分人执行操纵者的指令。

大部分人在想到婴儿时会微笑，在说到动物时会感觉“可爱”，我们甚至可能在想到某一流行产品时唱出它的广告歌曲。

这类战术很隐秘，很多时候我们甚至不知道它们已经在起作用了。很多时候我会想穿着暴露的比基尼女郎与啤酒有什么关系。

应用条件反射的一个例子是米其林轮胎。多年以来，这家公司一直在广告中使用婴儿（参见图6-12）。为什么？“因为轮胎承受了很多。”但是这些广告的含义更多。在看到婴儿时，你会微笑，会感到幸福。这种情感激发了一种正面的反应，这一反应让你欣然同意接下来要告诉你的内容。当看到婴儿时你会微笑，看多了以后，一看到米其林轮胎你就会有一种温暖、幸福的感觉。




图6-12　婴儿可爱吗

看到婴儿坐在轮胎旁，同样会让你对这一品牌有积极、幸福的感觉。这是一个操纵的经典例子。

百威啤酒的广告（参见图6-13）也很典型，很多人在想这则广告的含义——记得这些受欢迎的青蛙说出了“百”–“威”–“啊”吗？青蛙和啤酒有什么关系？循着这一思路，再想想最近的广告中出现的克莱兹代尔马和它的动物朋友。这些广告很引人注目，第一次看到的时候还会觉得滑稽，但是无法解释你为什么想买他们的啤酒。




图6-13　青蛙让销量大增

在这种形式的操纵里使用了隐秘的条件反射方法。看到这些广告时你会大笑，随后在开车去买啤酒时，看到厚纸板上的青蛙或骏马又笑了起来，这在你心中产生了积极的情感，让你愿意买这个牌子的啤酒。

以销售和市场为主导的公司经常会使用这种条件反射战术，目的是操纵消费者购买他们的产品而不是竞争对手的。社会工程人员并不销售产品，但想要目标“买”账，认同他们的伪装，采取他们期望的行动。但是为什么要使用操纵战术呢？使用这种强有力的控制方式有何好处？下一节将讨论这一话题。

## 6.4.5　操纵激励

操纵他人能够得到什么好处？这个问题直抵所有操纵方法、思维和战术的核心。并非所有的操纵都是负面的，但是都和其背后的激励有关。*激励*可能是正面的，也可能是负面的。

什么是激励？可以将激励看成刺激你采取行动的任何东西，比如金钱、爱、成功等，甚至是负面的情感，例如憎恨、嫉妒和羡慕。

人们选择操纵他人的主要原因可以分成三类：金钱激励、意识激励和社会激励。下面会逐个分析每一种激励以及如何将它们应用于操纵。

### 1. 金钱激励

金钱激励是最常见的，前面提到的例子大多和增加销售额有关。很多骗局的战术背后都有金钱激励的影子。

有多少人为了赢得大奖而每天买彩票？随着时间的推移，他们可能花了几百美元买彩票，但只要中20美元就会很开心，从而继续购买，希望能中更大的奖。

一个非恶意的金钱激励的例子就是优惠券。如果你在特定的商店购买特定的商品，就可以享受X美元X美分的优惠。如果你买东西时精打细算或者想要试用那个商品，就会去那家店。

很多商业机构在推销再教育、职业或技能培训时，会使用金钱激励的方法，为你描绘一幅画面：参加他们的课程和培训后，你的收入会大幅提高。

恶意攻击人员使用操纵战术的激励就是经济收益，因而他们的动机和技术也反映了这一点。例如，如果恶意社会工程人员的目的是让目标出让一部分辛苦挣来的钱，他伪装的角色将是“可以”要钱的人。在这种情况下伪装成慈善组织就比较合适，因为请求捐助或者询问财务信息是再寻常不过的事了。

### 2. 意识激励

意识激励非常难以描述。每个人的理想都不同，这些理想可以影响激励。如果你的理想是经营一家餐馆，那么这就是你的激情所在。你会长时间工作，比员工投入更多的精力，而且不太在意金钱回报，因为那是你的梦想和目的，而对其他人来说则只是一份工作。

梦想和信念可以深植于一个人的心中，以至于几乎不可能将它们同其人分开。当听到有人说“我有一个梦想”时，你会想到马丁·路德·金吗？有些人的梦想和目标是要成为什么样的人，而不是脑子中的空想。

人们会被拥有类似梦想和目标的人所吸引，所以“物以类聚，人以群分”这句话用在此处非常合适。但这也是很多人能够被操纵的原因。

让我们以基督教电视传道者为例来进行分析。那些信仰或者渴望信任上帝的人聚在一起。具有类似信念的人能够增强彼此的信念和做正确事情的欲望，但是电视传道者可以利用这种意识告诉他们上帝的意愿是让某个教堂繁荣，因而他们的钱包也就能鼓起来。

电视传道者进行几番激励性的布道、洒下一些泪水，突然间人们就将支票不断地送过来。这些传道者同时利用了金钱和社会理想这两种工具（参见下文），将听众的思维转换成他们的思维方式，所以这些人将辛苦挣来的钱捐了出来。有意思的是，如果你问那些追随者，对于“牧师比他们富裕得多”有何感觉，他们相信那是上帝的旨意。他们的思想已经发生了改变或者已经被操纵。

意识激励也能用于对人们进行道德教育，甚至借助恐惧这一激励方法也能对人们产生很大的影响。人们常常通过具有寓意的故事和寓言教育儿童意识激励。《格林童话》就是这种类型激励的最好例子。故事的结局通常是坏人受到惩罚或者死亡，而好人在坚忍不拔地克服各种困难后最终得到了巨大的回报。这些故事借助恐惧让孩子们知道做坏事会受到可怕的惩罚，甚至可能死去。

意识激励也用于市场营销，在"志趣相投"的人"碰面"的地方投放广告。例如，尿布公司在家庭杂志上做广告，动物保护组织选择在动物园做宣传，运动器材公司则瞄准体育赛事等。这种类型的激励使得广告中的商品或服务在具有共同思维模式的人群中热销。

意识激励用来让某人的思维与同类人结盟。通常，操纵战术开始于人们产生共鸣之时。同样，不是所有的操纵都是恶意的，但要以正确的方法使用。

### 3. 社会激励

社会激励也许是应用最广泛和最复杂的激励形式，特别是在社会工程活动中。

人类具有社会化的天性，这是我们通常的生活方式。社会激励包括所有其他类型的激励。适当的关系会提高你的金钱需求，也会调整、增强你的理想。可以说社会激励要比其他两种类型的激励更加强大。

很多人会受到来自同等地位的人的极大压力，这是显而易见的。对任何人来说，不论是年轻人还是老年人，随大流的吸引力都很大。很多时候，什么可以接受与社会激励直接相关。人们对生活和自身的看法，会受周围人群的极大影响。实际上，即使在没有直接同伴的情况下，也会感受到来自同伴的压力。

我好看吗？要看情况。如果我在美国，那里超级名模穿"零号尺寸"的衣服，男人身上都是肌肉，而我身上没有肌肉，那么我就不好看。如果我在古罗马，那里体格大就意味着富有和权力，那么我就好看。人们的内在自我会受到社会观点的影响。

1975年，美国空军进行了一项名为"空军技术训练中的社会激励鉴别和分析"的研究，尝试分析在训练和演习中培养领导者的社会激励效果。他们在小组中设置了4种不同的场景，分析其对学员的影响。

结果显示，一定的社会激励，通常包括来自同伴或权威人物的赞赏或正面支持，会在学员和教官之间建立起密切的关系。

> 整个研究的主要结论是社会激励的管理是一门艰难的艺术。虽然发现和调整社会激励很容易，但操纵和管理这些激励就难多了。实验数据显示了不同的社会激励的强大吸引力。实战实验的结果显示了熟人和心理契约训练对同伴学员态度的影响。这些发现强调了社会因素的重要性。

换句话说，当我们知道某个人的动力所在时，提高或降低社会激励的吸引力并不难。这种现象在少年中表现尤为突出。当发现他人的顾虑时，他们就可以将这一点作为武器逼其就范。施加压力的人越多，目标顺从的可能性就越大。

上面的句子要仔细琢磨。我同时也在想：如果研究者能够利用今天的众多社交网站，结果又会怎样呢？来自同伴的压力是一种强大的影响力，每个人都想成为大众中的一员。

社会激励很有效。2007年，奥丽埃纳・班迪耶拉（Oriana Bandiera）、伊万・鲍龙考伊（Iwan Barankay）和艾莫然・拉苏尔（Imran Rasul）合作发表了一篇研究论文Social Incentives: The Causes and Consequences of Social Networks in the Workplace，详见www.social-engineer.org/wiki/archives/Manipulation/Manipulation-Social-Incentivespdf.pdf。

这份报告讲述了一项很有趣的研究，该研究与空军的研究很像，只不过研究时间为2007年。基本上，研究者分析了那些在工作中有“朋友”的人，在与朋友一起工作时的情况。他们的结论如下。

> 我们的研究显示社会激励是真实存在的。在排除生产技术、补偿方案等可能带来影响的外部因素后，朋友的存在会影响工作者的效率。由于社会激励的存在，工作者在一起工作时会遵从共同的规范。朋友的存在会提高能力较差者的工作效率，反之，也会降低能力较强人员的工作效率。
>
> 社会激励对工作者的表现具有重要的决定作用。当工作者基于个人生产力按件计酬时，社会激励的表现会导致：(1)那些能力强的人会放弃10%的收入以遵从规范；(2)那些至少有一个比他能力强的朋友的工作者，会提高10%的生产力以符合规范。从总体上来说，工作者能力的分布是后者的影响占主导地位，所以社会激励对公司业绩的净影响是正面的。

朋友的存在意味着他们会更努力或者更放松。在没有外界压力的时候，来自同伴的压力会影响人们的工作效率。这种压力可以理解为标准。为什么？也许一个人能够工作得更快或者更好，但是他可能不想表现出什么都能干或者像拍马屁似的。如果平常比较懒散，他也不想显得懒惰，所以也会适当地更努力一些。不管是何种情况，他们的职业道德都会被朋友所影响。

管理的一个好策略就是总将工作最努力者和天生的领导者放到领头的位置。不过这个研究中还有很多可以学习的地方。

这个方法就是社会工程人员所用的“尾随战术”。混在一大群就餐或者休息回来的人中，装成其中的一员，在通过大门的时候一般保安都不会拦着。

这也是对整个人群进行操纵的方法，让他们认为某种行动或者态度是可以接受的。这一点你可以在娱乐圈中看到，每年可接受行为的标准和道德水平都在下滑，然而这种标准的降低通常打着“自由”的旗号。

实际上并不是只有这三种激励方法。它们可以分化成其他方面，这超出了本书的讨论范畴。不过我们仍然要分析一下社会工程人员怎样应用这些激励方法。

## 6.5 社会工程中的操纵

操纵并不是让人们喜欢你的所作所为并且感到舒服，而是强迫他们做你想要他们做的事。

强迫不是一个友好的词汇，它的含义是“迫使某人以某种方式行动或思考”或者“通过武力支配、阻止或者控制”。

操纵和强迫利用心理力量改变目标的观念、信仰、态度和行为。使用操纵和强迫的关键是通过一些不可察觉的小步骤逐步进逼。社会工程人员不想惊动他正在操纵的目标。下面的一些方法可能具有很大的争议或者很可怕，但是诈骗犯、身份窃贼等每天都在使用。操纵的一个目的是制造焦虑、紧张和过度的社会压力。当目标有这种感觉的时候，就更可能采取社会工程人员操纵他采取的行动。

通过以上内容，你就会明白为何人们常常对操纵持有负面的看法，但是由于其常用于社会工程中，因而必须加以讨论。

### 6.5.1 提高目标的暗示感受性

提高目标的暗示感受性通常会使用第5章中讨论的神经语言程序学技巧或者其他视觉提示。前面给出了一些例子，如通过钢笔的咔嗒声或者其他噪音或手势等让他人产生条件反射，甚至无需言语，就能诱发对方的情感。

我曾经亲眼见证过，当时一个人正在操纵目标，他使用钢笔的咔嗒声暗示一种积极的想法。他会说一些正面的东西，然后微笑并且让钢笔发出咔嗒声。慢慢地，在重复4~5次咔嗒声之后，我看到目标开始微笑。随后操纵者提到一个令人沮丧的话题，同时让钢笔发出了咔嗒声，结果目标首先开始微笑，然后立刻感到很尴尬。这种尴尬为操纵者打开了操纵目标的方便之门。

要制造一种他人易受暗示影响的场景，可以通过不断重复想法或者其他方法，使目标接受你的想法。

社会工程人员应该确保整个设置与操纵相配合，如使用的语句、描绘的画面和选择的服装颜色等，所有这一切会提高目标的暗示感受性。

威廉·萨金特（William Sargant）是一位有争议的精神病学家，也是《思维的战场》（*Battle for the Mind*）一书的作者，他谈论了操纵人的方法。根据萨金特的观点，用恐惧、愤怒或者激动等情绪扰乱了目标之后，可以为他植入不同的信念。这些情绪会导致暗示接受性提高和判断力下降。

社会工程人员可以利用这一方式达到自己的目的，首先给目标一个会令其感到恐惧或激动的暗示，然后提供一个解决方案，这个解决方案就是一条建议。

例如，在大受欢迎的BBC电视栏目《骗术真相》中，演员通过一场骗局演示了这种方法的可行性。他们在卖场中设置了一个摊位售卖奖券。购买奖券的人有可能获得三项奖品，其价值远高于所购买的奖券。

一位妇女购买了奖券，当然，她赢得了大奖。她的情绪异常激动，因为她之前从未获得过这样的大奖。此时，保罗・威尔森提出了一个建议从而操纵了她：在这种激动情绪之下，他告诉她必须拨打一个电话，并且需要提供银行信息以领取奖金。

她毫不犹豫地照做了。这个建议很合理，尤其是在她激动的时候。

了解目标、他的喜好、小孩的姓名、钟爱的球队和食物，然后利用这些制造一个易动感情的环境，就会轻松营造出易于接受暗示的气氛。

### 6.5.2　控制目标的环境

控制目标的环境通常用于在线社会工程、欺诈和身份盗用等场景。

成为同一社交网络和组织的一员，会让攻击者有机会获得操纵目标行动或思维的“会面时间”。如果能够利用目标的社交网络找出他们的情感触发点，效果也很不错。

在一次为客户调查非法诈骗犯的详细联系信息时，我使用了这种方法。在诈骗犯发布“战果”的论坛上，我找到了他的账号，然后进入了他的环境，成为了他的朋友，赢得了他的信任，通过社交网络了解他正在做的事情，最终获得了他的联系信息。

任何用来控制目标环境的方法都可以用在操纵战术中。控制目标环境可能简单到在不打扰目标时接近他，或者让目标看到或者看不到某一可能引起他反应的事物。

当然，除非你计划将目标带入黑暗的密室中，否则并不能真正控制他的整个环境，所以要想尽量控制就需要进行计划和研究了。在找到目标的社交圈子之后，不管是网络世界还是现实世界，你都要花时间设想一下如何进入并控制那个环境。一旦进入，你要控制什么呢？优秀的社会工程人员不会一上来就追求那“致命一击”，而是会慢慢建立关系、获取信息，然后才进行最后一击。

环境控制常用于警察或者战时审讯。审讯环境设置的气氛会让目标感到放松、紧张、害怕、焦虑或者审问者（或者军官）想让目标感到的任何情绪。

### 6.5.3　迫使目标重新评估

逐渐削弱目标的信念、意识或者对某一情形的情绪控制会让他不安。这一战术具有很强的负

面效果，因为它让目标怀疑他通常认为是对的东西。

邪教组织使用这一战术蚕食那些寻找人生方向的人。感觉迷失或者困惑时，人们常常认为需要重新评估自己的整个信仰系统。当邪教组织获取控制权时，他们会非常有说服力，受害者会彻底相信他们的家人和朋友不知道什么才是最好的。

在个人社会工程层面，你可以让他人重新评估以前被灌输的有关安全的理念，或者什么是公司政策、什么不是。

社会工程人员每天使用相似的战术，提出经过周密思考的问题，让目标重新评估其对某一问题的立场，动摇其信念。

例如，在当前的经济环境下，销售人员渴望提高销售额，也许公司对不经过扫描并采取防范措施就从网上下载PDF文件有严格的限制，但你还是可以致电公司的销售部门，说："你好，我是ABC公司的，想订购你们的产品，可能会超过10 000件。公司要求我获取三项报价，看看双方怎样合作比较好。我已将询价文件上传到了我们公司的网站上，我能将URL发给你吗？两个小时后我要去开会，你能看一下询价文件，在我开会前给出一份基本报价吗？"

你认为这一战术会成功吗？销售员很可能在稍加迟疑之后或者毫不犹豫地就下载并运行那个文件。你迫使他重新评估公司制定的政策。

### 6.5.4 让目标感到无能为力

让目标感觉脆弱或者无能为力是另一种阴暗但很有效的战术。它常用于社会工程，社会工程人员可以伪装成愤怒的主管或者其他比目标职位高的人。攻击者因目标没有反应或者不能快速回答问题而感到愤怒，于是严厉责备或者威胁目标，迫使他怀疑自己的立场，让他感觉无能为力。

另一种更加微妙的方式是通过社会激励逐渐削弱其信念系统。在一次审计中，我正在对内部网络进行扫描，管理员出面阻止了我。当她理直气壮地阻止我的时候，我的反应是："你知道这家公司每年得处理多少网络入侵事件吗？我在为你们进行安全加固，而你却阻止我工作！"

我的强势让她感觉无能为力，终于败下阵来。

让目标感觉没有时间思考或者情况特别紧急，也会让他觉得无能为力。他没有时间思考怎样处理问题，因此必须立刻作出一个决定。

在最近的海地地震发生后，有人利用了这一战术。有人创建了一个网站，声称上面有可能在地震中失踪的亲人的信息。因为他们声称除了建立网站的人之外，没有人可以提供他们失踪的亲人的信息，所以他们可以要求只有达到特定标准的人才能获取信息。很多觉得没有希望、无能为力的人，提供了太多的信息，点击了他们自己也知道不该点击的内容，结果最终被利用了。BBC发表了这一故事，并列出了一些保护自己的建议，详见http://news.bbc.co.uk/2/hi/business/8469885.stm。

### 6.5.5 给予非肉体惩罚

与让目标感到无能为力这一战术密切相关的就是让他们觉得内疚、耻辱、焦虑或者丧失特权。这些感觉非常强烈，目标可能会做任何事来“重获青睐”。

如果没有达到别人的期望会觉得丢脸并对自身产生怀疑，这会使得目标按照攻击者想要的方式作出反应。

我并不建议在大多数社会工程场景中应用耻辱这一策略，但是我曾经见过一个社会工程团队将其用在了一个目标身上，也用在了另一个社会工程小组成员身上以“软化”目标，使得他们更容易接纳别人的建议。

第一个攻击者接近处于公共环境中的目标尝试获得信息，他伪装成了一个重要人物。

在对话过程中，一名女性下属（也是团队成员）走向前问了一个问题，激怒了第一个攻击者。他的回应是：“你一定是我见过的最愚蠢的人。”说完，愤怒的他走开了。女性攻击者看上去很沮丧也很受伤，目标很快就开始安慰她，想让她心里好过些。目标的同情给了攻击者操纵他的机会，让他泄露出本不想泄露的更多信息。

### 6.5.6 威胁目标

威胁也许不是我们设想的传统意义上的社会工程会使用的战术。你不会将目标绑起来用“杰克·鲍尔”[①]的方式对待他，但是可以使用隐晦的方式进行威胁。

暗示目标不能照办的话会被解雇或者造成其他不利后果，就是对目标的一种威胁。政府常常会使用这种战术操纵社会大众相信经济体系正在崩溃，这样他们就能控制那些被统治的人的情绪。

甚至可以在社会工程审计中通过表现出一种威胁的样子来达到效果。看起来很忙、心烦、身负重任会威胁到不少人。如果在谈话中显露权威的表情也能对人产生威胁。

在商业活动中，通过认证的邮件或者快递发送物品隐含一定程度的威胁。让人签收内容不明的包裹，会让一些人感觉受到了威胁。这种操纵战术的目的就是要让目标觉得不自在和忧虑，这会让他做出以后会后悔的事情，但为时已晚。

社会工程和专业审计人员使用这些更为阴暗的操纵技术时得心应手。如果让目标觉得完全无能为力，他就会认为向攻击者屈服是相当合理的。

这是社会工程实践中的操纵和其他形式的影响战术的真正区别所在。在使用负面的操纵战术

① 杰克·鲍尔是美国电视剧《反恐24小时》中的人物，是一名非常有能力的联邦特工。——译者注

之后，社会工程人员丝毫不顾目标的感受就离开了。如果目标后来意识到自己被利用了，也不要紧，因为破坏已经造成，公司或个人已经被渗透了。

社会工程操纵的其他方面一样很有用，但不是这么阴暗。

### 6.5.7　使用积极的操纵

积极的操纵与消极的操纵目的相同，即最终目标的想法和愿望与你的达成一致。区别则在于实现结果所采用的方式不同。在积极的操纵中，目标在你达到目的后不需要心理治疗。

通过多年的研究，我总结了一些关于父母如何与儿童沟通的建议，以便让他们顺从父母的意愿。其中有几点是关于积极操纵的，对社会工程人员会很有用。下面讨论这些积极的技术。

#### 1. 不要让目标的表现影响你的情绪

不要让目标的表现影响你的情绪，这点非常重要。一旦让你的情绪介入其中，就是目标在操纵你了。你当然会产生情感，但是要控制自己的感觉并注意表露感情的方式。

你不能失去控制。你也要尽量控制负面情绪，这样才能始终控制局面。

控制你的情绪也会让目标感到放松。但这不是说完全不表露情感，那样也会让人不舒服。如果某人真的心烦，表现出适当程度的关心是好的，但是如果显露出太多的情感，就会让目标偏离方向，导致整个行动的失败。

保持情绪与伪装一致。如果你能控制情绪，就能始终控制住局面。优秀的社会工程人员能够做到忽略目标的行为和态度。如果目标表现出不安、生气、好战、粗鲁或者其他负面情绪，优秀的社会工程人员应保持平静、冷静和镇定。

#### 2. 寻找积极的话题

只要有可能，说个笑话或者称赞某物，但是不要显得怪异。你不能在走近门卫的时候说：“两个尼姑走进一间酒吧……”这个方法很可能不会奏效。同时，你也不能走向前台直接说：“哇，你真漂亮！”

寻找积极的话题能让所有人感到自在，但是必须适当、有涵养、有品味。以前面接近门卫的例子来说，在自我介绍后，可以赞美一下她孩子的照片：“哇，她真可爱！多大啊？4岁还是5岁？我也有个女儿。”这样做有助于后续计划的进行。

#### 3. 假定，假定，假定

你可能听别人谈起过有些人喜欢假定或者设想，但是在这里，请假定一切。假定目标会依照你想要的方式行动，假定他会回答你想知道的问题，假定他会同意你的所有要求。

假定你要问的问题以及要做的陈述。

“当我从服务器机房回到这里……”

这种表述假定你属于那里，并且已经具有访问权限。就前面提到的门卫的场景来说，在赞美之后可以继续说：“在检查完服务器回到这里时，我给你看一下我女儿的相片。”

假定你想要的会发生也大有好处，因为它会影响你的精神面貌。你必须从精神面貌上表现出你会得到想要的，这种信念会制造出新的肢体语言和面部表情，从而让你更好地伪装。

如果觉得会失败，你就会失败或者至少会影响你的肢体语言和面部表情。如果你的精神面貌是一切顺利，就真的会一切顺利。不过要提醒一句，千万不可自大。

例如，如果你心想“我当然稳操胜券，因为我很了不起，我是最好的”，这会影响你的表现，让目标失去兴趣。

#### 4. 尝试不同的开头

通常交流时都以标准的为什么/什么/何时作为开头，但是也可以尝试不同的方式，看看效果如何。一个流行约会网站www.okcupid.com的研究小组对数据进行整理后发现，非传统的开场白具有一定的价值。

记得前面关于赞美的讨论吗？OkCupid网站的研究小组发现，开始时恭维太过会起到与设想相反的效果。性感、美丽、热辣等词语的效果极差，相反，酷、棒极了、迷人等词语的效果更好。

研究小组发现，在通常的问候语中，“嗨”、“嘿”、“你好”等会让目标觉得平淡，不会被激起兴趣，而“最近怎么样”、“最近可好”、“你好啊”以及“哈罗”等则是更好的开头。

当然，这些是关于约会的统计，但我们要学习的重点是人们针对非传统的问候会给予更好的反馈。

同样，在社会工程场景中，使用不同的接近方法，你会注意到目标对信息的反应程度会有所提高。

#### 5. 使用过去时

当想表达负面情况并且不想让目标重复时，就用过去时。利用这一技巧，可以将过去的负面态度和行为放到他的回忆中，给他一个“重新开始”的机会，让他为你做一些好事。例如：

“当时你说我不能进去找史密斯先生……”而不是说：“你说我不能进去找史密斯先生时……”

虽然只是改变了时态，但效果截然不同。前者给人的印象是该情况发生在很久以前，让我们翻到改进的、崭新的一页吧，而且它也能让目标觉察你当时的感觉。

#### 6. 探讨并摧毁

计划一下怎样处理破坏性或者负面的态度和行为。设想你伪装成技术支持人员，想要进入服务器机房。通过之前的电话交流，你了解到每天上午10点会有一群人出去抽烟。你认为人们不断进出的时候是一个好时机。你准备好了一切，但是在进大楼的时候，前台刚刚得到一些坏消息，情绪很不好。你应该计划好了如何处理这种糟糕的情况。

如果不事先思考如何处理潜在的交流障碍或者破坏性影响，而是等到临场发挥，则大多数情况下会出现问题。这就提出了一种有趣的想法。你必须在行动之前就像目标一样思考：他会提出什么异议？当不认识的人打电话或走过来时，他会说什么？他会提出什么异议？他会是什么态度？仔细考虑这些事情能够帮助你制定出针对这些潜在问题的解决方案。

将你的想法和目标的潜在问题写下来，然后开始演练。让你的配偶或朋友扮演不友好的门卫或者警卫。当然，他们不能模仿出面部表情等元素，但是你可以为他们提供一个拒绝交流时可能出现的情况列表，以测试你的反应。

不断练习，直到你能自如地应对，但是不要照本宣科。要记住，僵硬和死板的应对会让你很难随机应变。

积极的操纵对目标具有非常大的影响，不仅不会让他觉得受到冒犯，而且在操纵得当的情况下，会让他觉得自己做了一件好事，从而有一种成就感。

## 6.6 小结

操纵是社会工程和影响力中的一个重要部分。本章涵盖了世界上最有智慧的人们几十年来对人类行为领域的研究成果。

对操纵他人这一想法的常见反应可能是：

- “我不想操纵他人。”
- “学习这个是错的。”

这两种意见代表了大多数人对操纵一词的看法。但愿你现在相信操纵不总是黑暗的艺术，它也能用在好的方面。

今天，一些最聪明的心理学家和研究员剖析、研究、分析了影响力。我正是基于这些研究才写出了本章的内容。例如，框架部分一定会改变你和他人交往的方式，回报会让你像社会工程人员一样思考，让你知晓如何利用影响。影响力是一个令人惊异的话题，有关这一主题的书籍有很多。

理解什么会触发目标想要采取某一行动，并让目标觉得这一行动对他来说有好处——这就是影响力的用途。

本章分析了人们行动的心理学和科学基础，并且阐明了社会工程人员是如何应用影响力的。

请记住，影响力和说服的艺术是让他人想要按照你设想的方式去做、去反应、去思考或者去相信的过程。

上面这句话体现了社会工程和操纵的精髓。它是变动任何框架的关键，是打开操纵之门的关键，也是成为影响力大师的关键。

社会工程人员也可以借助很多实物工具，有些看起来就像是电影《007》中用到的。我们将在下一章讨论社会工程工具。

第 7 章

# 社会工程工具

人是使用工具的动物，没有工具，一事无成；有了工具，无所不能。

——托马斯·卡莱尔（Thomas Carlyle）[1]

工欲善其事，必先利其器。工具是否合适将直接影响社会工程人员的能力和成败。然而，仅有工具还远远不够，还得知道如何熟练地使用工具，这样才能取得成功。

本章将讨论物理工具、电话工具以及基于软件的工具这三者之间的区别。需要注意的是，仅仅拥有最昂贵或最好的工具，并不会使你成为一名社会工程人员。工具在安全审计实践方面的作用，就如同菜肴中的调味品，放得恰到好处便成就美味佳肴，太多或太少则会造成味道太重或淡而无味。你一定不希望自己在执行社会工程任务时看起来像个腰间缠满工具的蝙蝠侠，同样也不愿意面临到了目标的门口却因缺少适当的工具而无法进入的窘境。

社会工程工具的范围十分广泛，本书并非教你怎样开锁或篡改来电显示，而是要为你提供足够的信息，来帮助你决定什么样的工具可以增强你的实战能力。

本章首先着重介绍开锁器、垫片和摄像机等工具。市场上一些新颖奇特的工具会让平凡的社会工程人员感觉自己就像是詹姆斯·邦德。本章将介绍一些这样的工具及其使用方法，同时展示一些工具的图片。此外，本章还会讨论社会工程攻击中如何篡改来电显示，介绍市面上几款最好的基于软件的信息收集工具，最后还将探讨一些密码分析工具。

① 托马斯·卡莱尔（1795—1881），苏格兰评论家、讽刺作家及历史学家。——译者注

# 7.1 物理工具

物理安全是指企业或个人为保障安全所采取的不涉及计算机的措施，通常涉及锁、摄像机及窗户传感器等工具。懂得物理安全并知晓其运作原理是成为优秀社会工程人员的前提之一。你不必精通这些装置，但要对目标所使用的安全机制有清晰的认知，这样能帮助你克服社会工程审计过程中的阻碍，走向成功。

## 7.1.1 开锁器

在讲开锁之前，我们先来了解一下锁的基本工作原理。

图7-1是简易弹子锁的简单示意图。

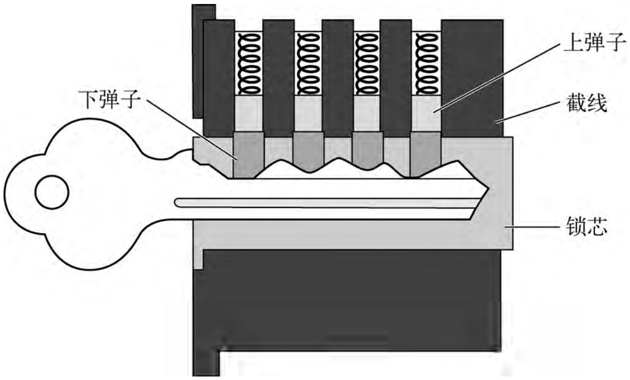



图7-1　弹子锁的简单示意图

弹子锁的基本工作原理是通过钥匙控制弹子。钥匙将下弹子和上弹子推至一定的高度，当两类弹子的截线正好与锁筒和锁栓之间的缝隙一致时，便可以轻松地转动钥匙打开门、服务器机房及陈列柜等。

开锁器模拟了钥匙将所有弹子一个接一个地移动到正确位置的过程，使得锁芯可以自由转动并打开门。开锁时，所需配备的两个主要工具是拨片和扭力扳手。

*拨片*是末端弯曲的长金属片，类似于牙医的工具。使用时将其插入锁的内部，上下拨动弹子直至其处于正确的位置。

*扭力扳手*是小而扁的金属器具，当使用拨片时，它能向锁施加压力。

*耙子*的外形很像拨片，但它用于在锁上“耙”动以操作所有弹子。耙子可以十分迅速地打开大部分锁，这一特性对开锁者极具吸引力，因为这样的话，大部分锁就可以被快速打开了。

要开锁，请遵循下列步骤。

(1) 将扭力扳手插入锁眼，沿着用钥匙开门时转动的方向扭转。关键技巧是知道施加多大的张力，因为力太大或太小，弹子都不会进入正确的位置，从而无法打开锁。若用力恰到好处，则会创建一个小平台，从而让锁芯能卡住销轴。

(2) 插入拨片，一个接一个地拨起弹子，直到感觉它们都处在固定的位置上了。当上弹子就位时，能听到轻微的咔嗒声。所有的弹子都就位后，锁芯便可自由地旋转，锁也就打开了。

上述步骤只能说是开锁的皮毛。欲了解更多有关开锁的知识，请访问下列网站。

- http://toool.us/
- http://home.howstuffworks.com/home-improvement/household-safety/security/lock-picking.htm
- http://www.lockpicking101.com/

这些只是众多致力于开锁教学网站的冰山一角。作为一名社会工程人员，花时间练习开锁是明智的。当需要的信息被锁在服务器机柜、书桌抽屉或者其他设备中时，随身携带的小型开锁套装可能就成了你的制胜法宝。

开锁套装可以很小，图7-2中所示的开锁器只有普通名片大小。

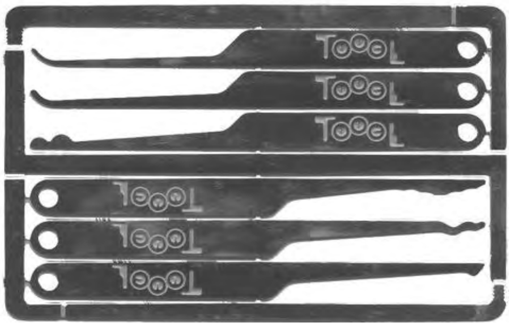



图7-2　这种名片大小的开锁套装很适合放在皮夹或钱包中

不过有时开锁套装也会比较大，就像图7-3和图7-4展示的那样。




图7-3　这套跟随身小折刀的尺寸差不多



图7-4　该开锁套装比较大，所需工具一应俱全

敬告：要在关键时刻来临前学习使用开锁器。就个人而言，我先买了一些不同尺寸的玛斯特（Master）牌的挂锁。成功地将它们全部撬开后，我又买了一套如图7-5所示的万能钥匙。它们适用于不同弹子类型的锁。弹子类型多样，这无疑会增加开锁的难度。持有不同弹子类型和不同大小的万能钥匙，能使你的练习实现最佳效果。

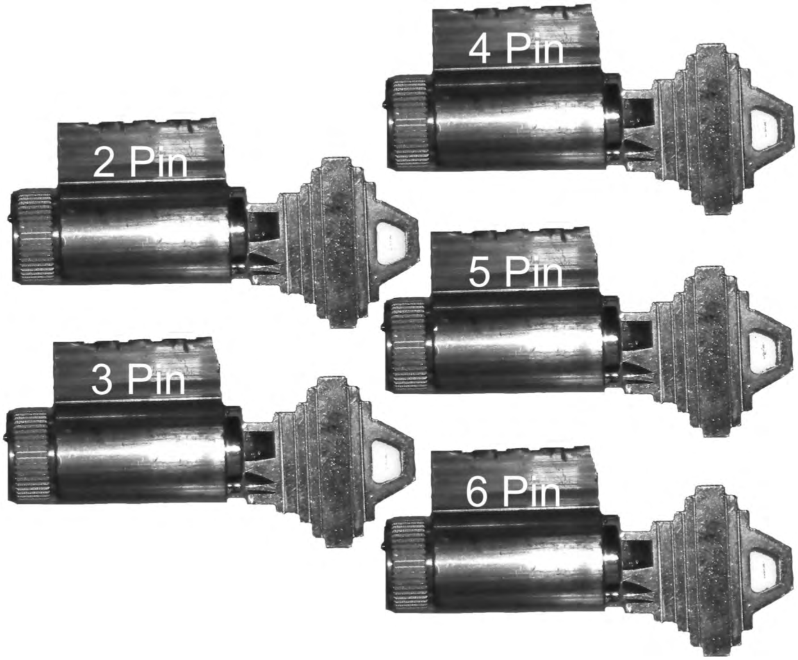



图7-5　这些透明的锁可以让你看到整个操作过程

我甚至在会议上见过一些极其精巧的装置，它们就像一个自制的锁墙，值得研习。当然，在收集目标信息的时候，拍摄或记录需要打开的锁的类型、品牌和具体型号，也是个不错的主意。了解这些信息能够为你的社会工程实践做好铺垫。

### 1. 实际应用

在电影和电视描绘的撬锁场景里，某人只要将开锁器插进锁眼中，短短几秒钟，门就奇迹般地打开了。或许某些人的开锁技能确实很高超，但是大多数人的成功之路很漫长，在经历了无数次的失败和挫折后，他们才能真正掌握撬锁和耙锁的技巧。耙锁本身就需要一定的天赋，关键在于使用耙子轻轻地在锁中耙进耙出的同时对扭力扳手施加些许压力。这一简单的方法可以撬开多种类型的锁。学会耙锁后，社会工程人员就知道如何正确地使用扭力扳手了，并能体会锁被撬开时的感觉。

许多公司开始采用射频识别（RFID）、磁卡或其他类型的电子准入技术，这可能让人觉得开锁技术已经过时了。实则不然，锁还在用，开锁技术也仍有用武之地，说不定哪天这项技能就能救你于水火之中。

下面的案例就充分体现了随身携带开锁器的好处。在一次行动中，我遇到一个无法使用社会工程方法来解决的障碍——一扇门。拔出一向值得信赖的袖珍开锁器，使用耙的方式，大约30秒钟之后我就成功进门了。很多社会工程人员都有过类似的经历，懂得锁的原理并携带适合的工具才造就最终的成功。公司会花费数万甚至数百万美元购买硬件、防火墙、入侵检测系统以及其他保护手段，再把它们都扔在一个房间里，最后只用廉价的玻璃和一把20美元的锁来保护它们。这样的情况屡见不鲜。

因为撬锁会面临被发现或被抓住的风险，所以练习是必不可少的。你必须动作迅速以降低风险。有些地方安装了摄像头来监控这种行为，但最终效果不佳，除非当时有人正在监视摄像画面，否则它只是记录了有人非法闯入并窃取服务器的过程而已。

通过一些简单的手法就可逃过摄像头的法眼，比如用LED强光照镜头或者用帽子或头巾遮住面部。

### 2. 打开磁性锁和电子锁

磁性锁之所以越来越风靡，主要原因在于其运行费用低廉并且提供了一定程度的安全保障，不像传统的弹子锁那样可以被撬开。磁性锁的形状、大小和磁力级别各异。只是从某种程度上来讲，磁力锁也并不安全：如果突然断电，大部分磁力锁将失效，门就被打开了。当然，没有使用后备电源才会产生这样的后果。

强尼·龙是世界知名的社会工程人员和黑客，谷歌黑客入侵数据库的创始人及《非技术黑客》（*No Tech Hacking*）一书的作者。他讲述了自己使用衣架和毛巾绕过磁性锁的故事。他注意到员工从里向外走向门口的动作会触动门锁打开，还注意到门中间有一道足以塞进一个系着毛巾的衣架的间隙。通过摇动毛巾，锁就被打开了，他也就长驱直入了。

我最近实践了一下这一过程。果然只要略微施力，并确定所需衣架的长度，两分钟不到我就

打开了锁。最让人惊讶的是，即便花大价钱安装专业的商务锁、配备防弹玻璃的金属门，同时增加后备电源和断电的情况下自动上锁的栓锁，也防不住衣架和破布。

当然，打开这些锁也可采用一些高科技的方法。有人发明了RFID克隆机，该小型设备可通过获取和重放RFID密码打开门锁。市场上也有多种复制磁性卡的设备。

### 3. 各种各样的开锁工具

除了扭力扳手和拨片之外，社会工程人员可能也会使用一些其他的工具（比如推刀、撞匙和挂锁垫片等）来进入目标地点。掌握了下列工具的使用技巧后，就可以轻而易举地进入目标场所了。

(1) 推刀

推刀被誉为最快捷的打开旋钮锁门的工具，如图7-6所示。旋钮锁常用于服务器机房或办公室的门。这把刀基本上可以在不破坏门的情况下切进正确的位置释放门闩。

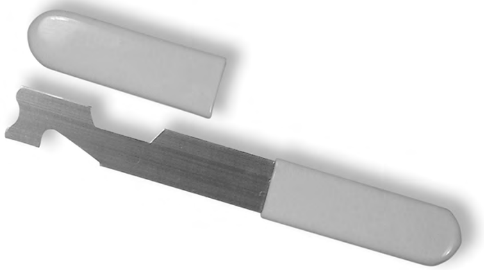


图7-6 典型的推刀

(2) 撞匙

虽然撞匙已经面世多年，但只是因为被用于犯罪行为才在新闻中被广泛关注。撞匙是经过特别设计的钥匙，用户把钥匙插进锁里，轻轻用力使之在适当的位置发生“碰撞”，将所有的弹子排成一条线，这样就可以在不破坏锁的情况下，转动锁芯。基本的技巧是把钥匙插入锁中，拔出一个或两个凹口的长度，然后对钥匙稍稍用些力，用螺丝刀或其他小物体轻轻“碰撞”钥匙。这个动作强行使弹子进入恰当的位置，这样锁芯就可转动了。图7-7展示的就是一把撞匙。



图7-7 典型的撞匙

(3) 挂锁垫片

垫片是插入挂锁底部的一小块薄金属片，用来解除锁定机制。垫片被推入底部的锁轴，将锁轴与锁定机制分开，然后解开锁。如图7–8所示。

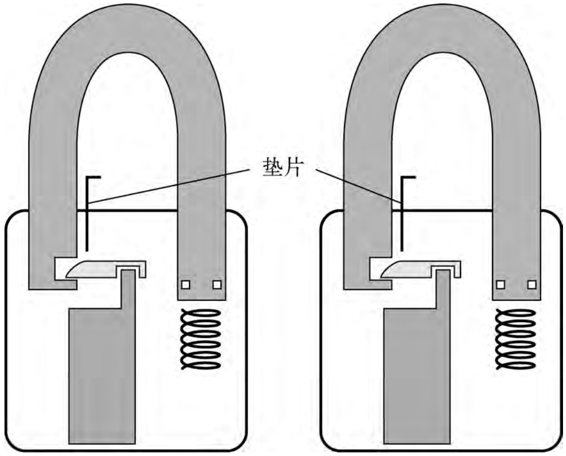



图7-8　垫片的工作原理

图7-9展示的是专业的垫片，也可用铝罐制作。



图7-9　专业垫片

近期发生的故事（参见www.youtube.com/watch?v=7INIRLe7x0Y）表明要打开宾馆或者配有链锁的房门简直易如反掌。侵入者在锁链上系上橡皮圈，利用橡皮圈本身的弹力，就可以使链锁脱落。麻省理工学院提供了一个自由发布的开锁指南（详见www.lysator.liu.se/mit-guide/MITLock-Guide.pdf），其介绍更为深入详尽。

你或许会好奇是否存在这样一种锁，它不会被撬开或至少很难被撬开。防撬双锁（Bump Proof BiLock，参见www.wholesalelocks.com/bump-proof-bilock-ult-360.html）就是这样一种锁。双锁孔设计使得它几乎不可能被撬开。

我在职业生涯中，遇到的不是锁的选择问题，而是与锁相关的安全问题。通常情况下，公司

会买一把结实的锁，需要生物识别技术和密钥才能进入服务器机房，但门旁边就是一个单层玻璃的小窗。那么谁还需要开锁器呢？贼可以轻而易举地打破玻璃闯进去。

其寓意在于单凭锁是无法保证安全的。安全是一种意识，而不是一种简单的硬件。

不是每个社会工程人员都必须成为开锁专家，但是知晓锁的基本工作原理并具有开锁经验，可能会影响社会工程行动的成败。

以上只是简单地讨论社会工程人员可能使用的开锁工具。另一个对社会工程人员具有非凡价值的工具是录音录像设备，详见下一节。

### 7.1.2　摄像机和录音设备

摄像机和录音设备似乎常与“偷窥”联系在一起，所以问题就来了：“为什么？为什么要在社会工程活动中使用针孔摄像机和隐蔽的录音设备？”这个问题提得好，答案很简单：为了证据，也为了自我保护。

我们先来讨论*证据*的概念。正如前面提到的，社会工程审计是对人进行测试。它是试图帮助一家公司修补基础架构中由人造成的薄弱点，从而提升安全性。不过恶意社会工程入侵者也可能使用相同的方法。许多人不愿意承认自己会被骗，除非证据确凿或者看到同事被骗。人们之所以不愿承认，究其原因可能是因为被社会工程人员欺骗而难堪，亦或是担心老板知道后的反应。录音设备可以提供证据，也可以据此对审计人员和客户进行培训。

使用这些设备的目的不能是让对方员工陷入困境或使其窘迫。不过，这些设备记录的信息会成为以后绝好的学习素材，可以展示员工是怎样认同社会工程人员所伪装的角色的。证明攻击会成功只是第一步，培训公司及其工作人员如何应对恶意的社会工程攻击（即如何注意、避免或者减轻这种攻击）还有很长的路要走。

社会工程活动中使用录音录像设备的第二个原因是为了自我保护，这主要针对专业的社会工程人员。为什么？仅凭肉眼观察并记录稍后可供分析使用的每个微表情、面部表情和小细节是不可能的。摄像机捕捉到的很多细节都可用来详细分析，为后续的攻击做准备。录像设备可以记录并证明你做了什么、没有做什么，而且你也无需将一切都记忆在脑中。对于分析社会工程活动成败的原因，这也是个不错的教育工具。

这项原则被执法部门广泛采用。警察和联邦探员用它来记录交通拦检、会谈和盘问等证据，这些证据可以用于自我保护、培训和法庭证明。

这些原则同样适用于录音。录下通话或谈话内容与之前所说的视频记录的目的相同。这里必须提及的重要一点是，在很多地方，未经许可的录音行为是违法的。社会工程人员必须确保与公司签署的合同中规定了自己有合法使用录音设备的权利。

录音设备的形状和大小各异。我有一个小型录音器，是一支可以使用的钢笔。该装置恰好能放在胸前的口袋里，清晰记录声音的范围可达20英尺（约为6.1米）远。加上2GB的内存，我可以轻松地记录数小时的谈话，然后进行分析。

1. 摄像机

现在可以找到形状像纽扣和钢笔的摄像机，它们可以隐藏在笔尖、时钟、泰迪熊玩具、假的螺帽和烟雾报警器中，基本上能想到的任何设备都可以隐藏摄像机。要像图7-10那样安装摄像机已非难事。

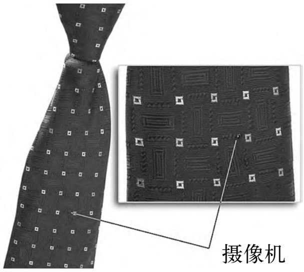



图7-10　隐藏在领带中的摄像机

信不信由你，这条领带隐藏着全彩摄像头，使用12伏电源，并连接一个小型录制设备。戴着这条领带进行社会工程审计，绝对可以录制70度视角以内的一切事物。

使用类似的录制设备好处多多，比如社会工程人员可以全力关注事先准备好的伪装或诱导方案，而不必担心遗忘任何细节。

关于录音设备的使用，我给大家讲个故事，是关于我对一个提供在线售票服务的主题公园进行的一次安全审计。这个公司开设了一个售票窗口，有一名女工作人员在里面操作Windows系统的计算机。我假装在酒店通过网络购买了入场券但是不能打印出来，于是将入场券转换成PDF格式的文件，并以邮件方式将其发送给自己。我对她说："我知道这个要求很奇怪，但是我女儿在一家餐厅看到了你们的广告，接着我们就立刻回酒店使用折扣码买了票，买完后却发现不能打印。酒店的打印机发生了故障，可我不想就这么浪费了入场券，所以把它们转换成PDF文件并发送到自己的邮箱中。您能帮我查看下文档吗？我自己登录也可以。""孩子"就等在一旁，当然，作为父亲，我不想让他失望。工作人员点击PDF的时候自然不会看到我们的票，而她的计算机已被恶意代码感染，这段代码能使我入侵她的计算机并开始自动收集信息。将谈话录音、我使用的方法以及设计的故事情节为该公司上了一堂课，以后碰到类似的情况就不再会被攻击了，从而避免了数千美元的损失。

一种使用现买现付充值卡的设备能通过手机信号给任意指定号码发送音频内容。社会工程人员可以随时拨入聆听录音内容。这个设备可用于在社会工程攻击中获取密码或个人信息，从而为社会工程人员节省了大量的时间。

人们可以花好几十个小时谈论各种精巧超酷的摄像机（我也可以写好几十页）。图7-11和图7-12展示了执法者普遍使用的一些“间谍装备”（www.spyassociates.com）。信不信由你，图片中的所有物品里都隐藏了摄像机或录音设备。可以使用其中任何一种设备秘密记录目标者的信息，以备分析。



图7-11　图中的笔可用来录音，其他物品都带有隐藏的具备录音功能的彩色摄像机




图7-12　这些物品也可通过隐藏的摄像头来录音录像

### 2. 使用工具

前面概述了一些不同类型的录音录像设备，但问题依旧是应如何使用。使用录音和摄像设备的基本原则与使用社会工程人员手中的其他工具（如伪装或诱导）是一样的。

最重要的还是练习。如果不能确定放置体载摄像机或录音设备的合理位置，最后可能只录到了天花板或者一段模糊的声音。准备并调校要携带的装备，并把摄像机和录音器放在适当的位置是很有必要的。试着坐下、起立、走几步，看看这些动作会不会影响音频和视频的质量。

从专业社会工程人员的角度出发，我必须再次强调合同中列出录音录像权限的重要性。如果没有合同许可，你可能会陷入法律困境。查阅当地的法规，确保使用这些设备不会惹来麻烦，也

是个不错的主意。

社会工程人员绝对不能使用这些设备故意去记录他人的窘态或窥探别人的隐私。

关于这个主题的讨论可以一直持续下去，希望本节对这些工具的概述及其使用方法的介绍能为社会工程人员打开一扇选择的大门。

下一节中，将给出社会工程人员可使用的另外一些工具的例子。

### 7.1.3 使用GPS跟踪器

社会工程人员通常想知道目标不在办公室时的行踪。目标在上班的路上做了哪些停留，能泄露很多信息。整合并分析这些信息有助于社会工程人员进行合适的伪装，或提出合适的问题，从而诱导目标作出正确的反应。知道目标一天工作的起始时间，对红队[①]的物理攻击也很有帮助。红队的目标是侵入并获取有价值的资产，用以暴露公司物理安全的脆弱性。

跟踪目标的方式多种多样，其中一种方法就是使用跟踪设备。GPS跟踪器是其中的一种，例如大家熟悉的可全球使用的SpyHawk超级GPS跟踪器，该设备可以从www.spyassociates.com网站买到。SpyHawk只是众多同类设备中的一种，售价大约为200~600美元。它能靠磁力吸附在汽车上，可以存储被跟踪目标好几天的信息。下面将讲述如何安装和使用这个小装置。

#### 1. SpyHawk超级GPS跟踪器

要安装设备附带的软件很简单。只需点击运行安装软件，按照屏幕上提示的步骤操作，就可以顺利安装成功。安装后，设置步骤也相当简便。如图7–13所示，跟踪器（TrackStick）的界面很直观，设置也很容易。

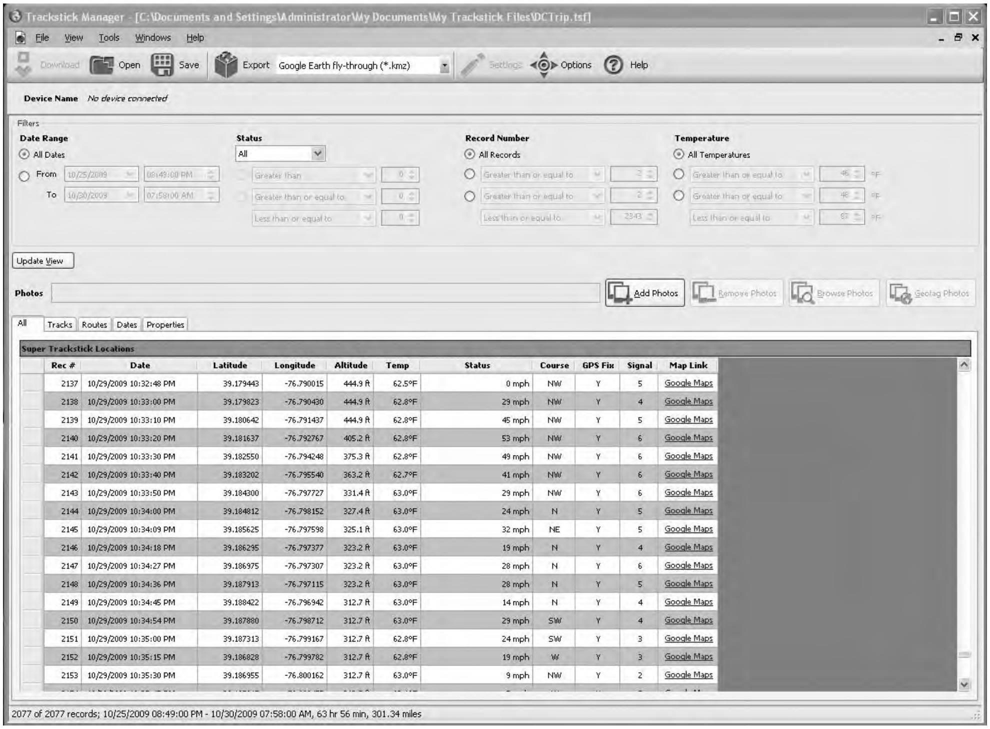
如图所示，它提供了日志条数、时区和更多的自定义选项。

#### 2. SpyHawk跟踪器的使用

SpyHawk超级GPS跟踪器很轻，易于使用和隐藏。它仅配备了一个开关键，但其中采用了一些精巧的技术。当它感应到移动时，会启动并开始记录。当移动停止一段时间后，它便停止记录。

说明书上说，该设备具有强磁性，可吸附在金属上以便隐藏，但不适用于表面粗糙或者表面是塑料的地方。第一次使用该设备时难免害怕丢失，因此在引擎盖下找到一个安全的位置，可以让人更安心，记录效果也更佳。当接近目标车辆时（无论是内部还是外部），轮舱、引擎盖下面或者后备厢等带有金属的地方都比较安全。如果你能接触汽车内部，打开引擎盖，将它放在里面，就更不用那么担心被发现或丢失了。

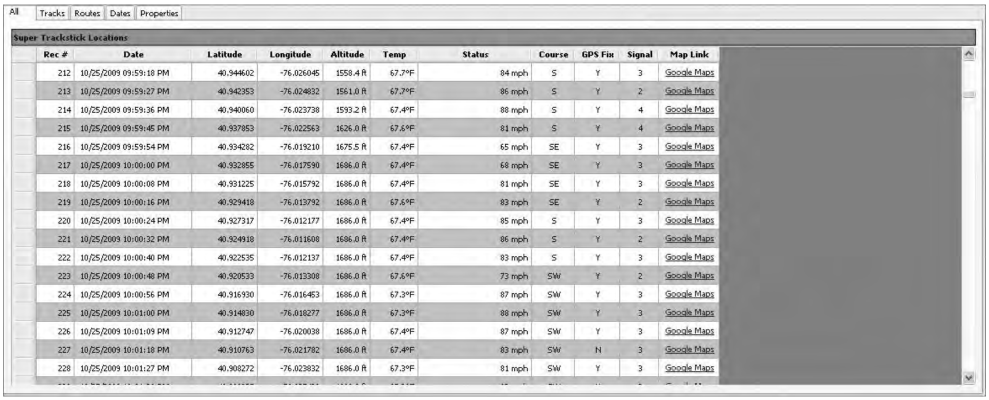
① 红队是指计算机和网络安全专家，他们得到系统主人的授权攻击系统，以找出恶意黑客可能利用的安全漏洞。也被称为伦理黑客、入侵测试等。——译者注




| Rec # | Date | Latitude | Longitude | Altitude | Temp | Status | Course | GPS Fix | Signal | Map Link |
|---|---|---|---|---|---|---|---|---|---|---|
| 2137 | 10/29/2009 10:32:48 PM | 39.179443 | -76.790015 | 444.9 ft | 62.5°F | 0 mph | NW | Y | 5 | Google Maps |
| 2138 | 10/29/2009 10:33:00 PM | 39.179823 | -76.790430 | 444.9 ft | 62.8°F | 29 mph | NW | Y | 4 | Google Maps |
| 2139 | 10/29/2009 10:33:10 PM | 39.180642 | -76.791437 | 444.9 ft | 62.8°F | 45 mph | NW | Y | 5 | Google Maps |
| 2140 | 10/29/2009 10:33:20 PM | 39.181637 | -76.792767 | 405.2 ft | 62.8°F | 53 mph | NW | Y | 6 | Google Maps |
| 2141 | 10/29/2009 10:33:30 PM | 39.182550 | -76.794248 | 375.3 ft | 62.8°F | 49 mph | NW | Y | 6 | Google Maps |
| 2142 | 10/29/2009 10:33:40 PM | 39.183202 | -76.795540 | 363.2 ft | 62.7°F | 41 mph | NW | Y | 6 | Google Maps |
| 2143 | 10/29/2009 10:33:50 PM | 39.184300 | -76.797727 | 331.4 ft | 63.0°F | 29 mph | NW | Y | 6 | Google Maps |
| 2144 | 10/29/2009 10:34:00 PM | 39.184812 | -76.798152 | 327.4 ft | 63.0°F | 24 mph | N | Y | 5 | Google Maps |
| 2145 | 10/29/2009 10:34:09 PM | 39.185625 | -76.797598 | 325.1 ft | 63.0°F | 32 mph | NE | Y | 5 | Google Maps |
| 2146 | 10/29/2009 10:34:18 PM | 39.186295 | -76.797377 | 323.2 ft | 63.0°F | 19 mph | N | Y | 4 | Google Maps |
| 2147 | 10/29/2009 10:34:27 PM | 39.186975 | -76.797307 | 323.2 ft | 63.0°F | 28 mph | N | Y | 6 | Google Maps |
| 2148 | 10/29/2009 10:34:36 PM | 39.187913 | -76.797115 | 323.2 ft | 63.0°F | 28 mph | N | Y | 5 | Google Maps |
| 2149 | 10/29/2009 10:34:45 PM | 39.188422 | -76.796942 | 312.7 ft | 63.0°F | 14 mph | N | Y | 4 | Google Maps |
| 2150 | 10/29/2009 10:34:54 PM | 39.187880 | -76.798712 | 312.7 ft | 63.0°F | 29 mph | SW | Y | 4 | Google Maps |
| 2151 | 10/29/2009 10:35:00 PM | 39.187313 | -76.799167 | 312.7 ft | 62.8°F | 24 mph | SW | Y | 3 | Google Maps |
| 2152 | 10/29/2009 10:35:15 PM | 39.186828 | -76.799782 | 312.7 ft | 62.8°F | 19 mph | W | Y | 3 | Google Maps |
| 2153 | 10/29/2009 10:35:30 PM | 39.186955 | -76.800162 | 312.7 ft | 63.0°F | 9 mph | NW | Y | 2 | Google Maps |

图7-13　跟踪管理器提供了直观易用的用户界面

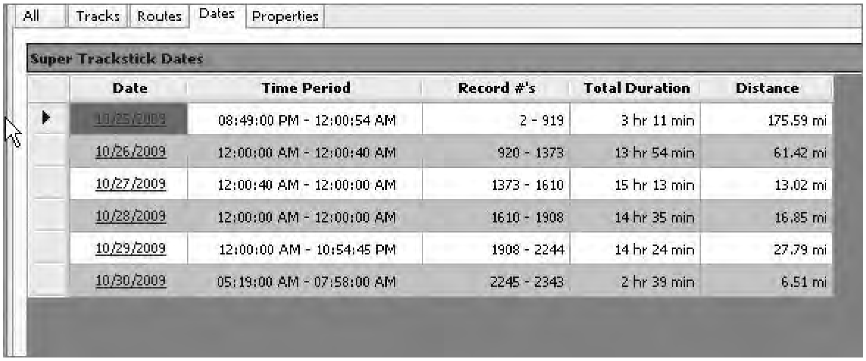
第一次测试时，我将装置放在了引擎处。即使是隔着金属引擎盖，记录质量也非常完美。另一个理想的做法是，等到目标汽车开锁后，将跟踪器放置在车厢内的脚垫下，或靠近尾灯的位置。根据我的记录，该装置在测试中收集了5天的数据，其中一些可以在下图中看到。如图7–14所示，看起来这个目标喜欢开快车。




| Rec # | Date | Latitude | Longitude | Altitude | Temp | Status | Course | GPS Fix | Signal | Map Link |
|---|---|---|---|---|---|---|---|---|---|---|
| 212 | 10/25/2009 09:59:18 PM | 40.944602 | -76.026045 | 1558.4 ft | 67.7°F | 84 mph | S | Y | 3 | Google Maps |
| 213 | 10/25/2009 09:59:27 PM | 40.942353 | -76.024832 | 1561.0 ft | 67.7°F | 86 mph | S | Y | 2 | Google Maps |
| 214 | 10/25/2009 09:59:36 PM | 40.940060 | -76.023738 | 1593.2 ft | 67.4°F | 88 mph | S | Y | 4 | Google Maps |
| 215 | 10/25/2009 09:59:45 PM | 40.937853 | -76.022563 | 1626.0 ft | 67.6°F | 81 mph | S | Y | 4 | Google Maps |
| 216 | 10/25/2009 09:59:54 PM | 40.934282 | -76.019210 | 1675.5 ft | 67.4°F | 65 mph | SE | Y | 3 | Google Maps |
| 217 | 10/25/2009 10:00:00 PM | 40.932855 | -76.017590 | 1686.0 ft | 67.4°F | 68 mph | SE | Y | 3 | Google Maps |
| 218 | 10/25/2009 10:00:08 PM | 40.931225 | -76.015792 | 1686.0 ft | 67.4°F | 81 mph | SE | Y | 3 | Google Maps |
| 219 | 10/25/2009 10:00:16 PM | 40.929418 | -76.013792 | 1686.0 ft | 67.6°F | 83 mph | SE | Y | 2 | Google Maps |
| 220 | 10/25/2009 10:00:24 PM | 40.927317 | -76.012177 | 1686.0 ft | 67.4°F | 85 mph | S | Y | 3 | Google Maps |
| 221 | 10/25/2009 10:00:32 PM | 40.924918 | -76.011608 | 1686.0 ft | 67.4°F | 86 mph | S | Y | 2 | Google Maps |
| 222 | 10/25/2009 10:00:40 PM | 40.922535 | -76.012137 | 1686.0 ft | 67.4°F | 83 mph | S | Y | 3 | Google Maps |
| 223 | 10/25/2009 10:00:48 PM | 40.920533 | -76.013308 | 1686.0 ft | 67.6°F | 73 mph | SW | Y | 2 | Google Maps |
| 224 | 10/25/2009 10:00:56 PM | 40.916930 | -76.016453 | 1686.0 ft | 67.3°F | 87 mph | SW | Y | 3 | Google Maps |
| 225 | 10/25/2009 10:01:00 PM | 40.914830 | -76.018277 | 1686.0 ft | 67.3°F | 88 mph | SW | Y | 3 | Google Maps |
| 226 | 10/25/2009 10:01:09 PM | 40.912747 | -76.020038 | 1686.0 ft | 67.4°F | 87 mph | SW | Y | 3 | Google Maps |
| 227 | 10/25/2009 10:01:18 PM | 40.910763 | -76.021782 | 1686.0 ft | 67.4°F | 83 mph | SW | N | 3 | Google Maps |
| 228 | 10/25/2009 10:01:27 PM | 40.908272 | -76.023832 | 1686.0 ft | 67.3°F | 81 mph | SW | Y | 3 | Google Maps |

图7-14　目标喜欢开快车

时间、日期和时长标记有助于你勾划出目标的行驶轨迹，如图7-15所示。


All | Tracks | Routes | Dates | Properties

Super Trackstick Dates

| Date | Time Period | Record #'s | Total Duration | Distance |
|---|---|---|---|---|
| 10/25/2009 | 08:49:00 PM - 12:00:54 AM | 2 - 919 | 3 hr 11 min | 175.59 mi |
| 10/26/2009 | 12:00:00 AM - 12:00:40 AM | 920 - 1373 | 13 hr 54 min | 61.42 mi |
| 10/27/2009 | 12:00:40 AM - 12:00:00 AM | 1373 - 1610 | 15 hr 13 min | 13.02 mi |
| 10/28/2009 | 12:00:00 AM - 12:00:00 AM | 1610 - 1908 | 14 hr 35 min | 16.85 mi |
| 10/29/2009 | 12:00:00 AM - 10:54:45 PM | 1908 - 2244 | 14 hr 24 min | 27.79 mi |
| 10/30/2009 | 05:19:00 AM - 07:58:00 AM | 2245 - 2343 | 2 hr 39 min | 6.51 mi |

图7-15　被跟踪目标的行驶轨迹

图7-16显示了信息在谷歌地球上的呈现，包括速度、时间、停止时间及其他信息。

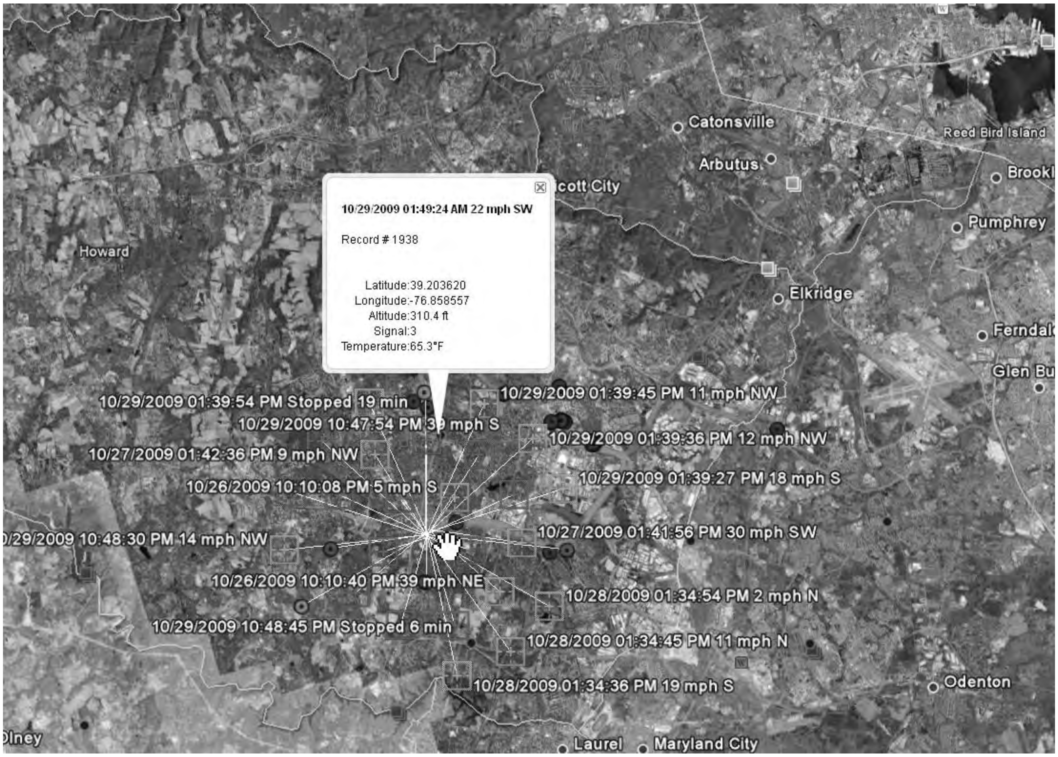



图7-16　装置提供谷歌地图输出

如图7-17所示，软件完美地展示了完整的线路图。




图7-17　跟踪器给出的目标行驶路径

利用谷歌地球或谷歌地图软件，可以放大查看细节（见图7-18）。

### 3. GPS跟踪器数据分析

跟踪器采集的数据对社会工程人员大有裨益。如果能够跟踪到目标公司的CEO每次喝咖啡的地方、最喜欢的商店以及健身会所等信息，将有助于社会工程人员作出成功率最高的攻击计划。

了解了目标的位置及停留的地方，攻击者就可以确定在何处复制RFID证件或者取得钥匙模印的机会最大。这样做的好处在于不必伪装成邻居悄悄靠近目标。下面的图片展示了攻击者如何利用这些细节占尽上风。




图7-18　放大目标移动的路线

请注意图7-19中的细节。你可以看到目标开车的速度以及停车的日期和具体时间。如果想看到其位置的更多细节，点击谷歌地图链接，点击“导出”按钮，将所有的数据集导出到谷歌地图或谷歌地球中。

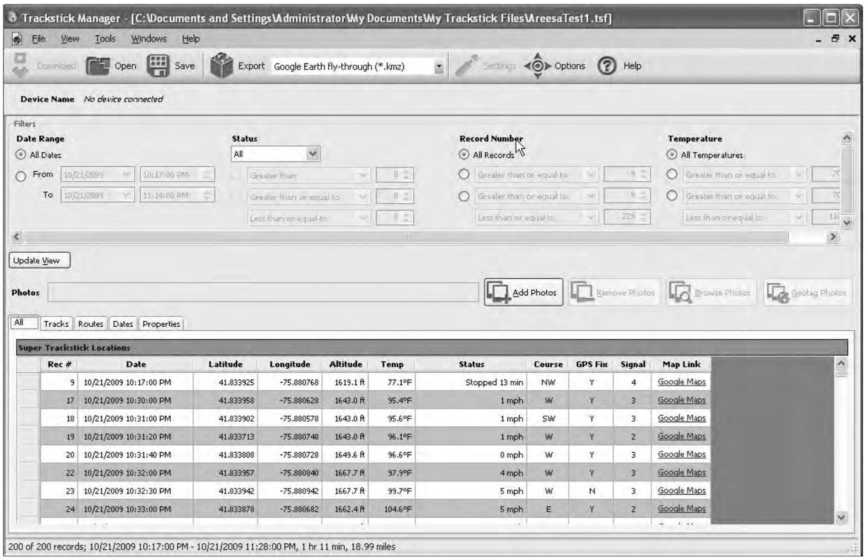



图7-19　数据集

在谷歌地球中打开数据集后，你可以看到他的停车点、行驶的路线以及停下的次数等，如图7-20所示。

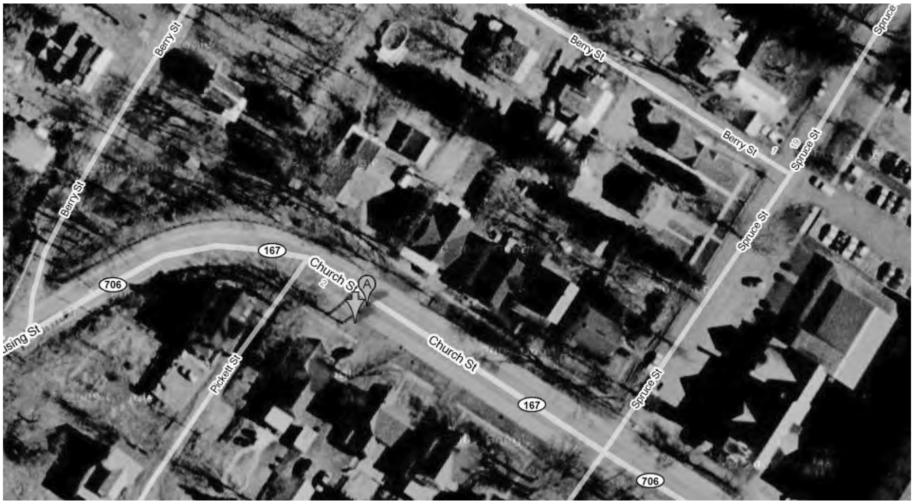



图7-20　路程中的暂停点

如果你想看他的整个行驶路线，没有问题，只要从众多格式中选择一种输出整个路线，如图7-21所示。

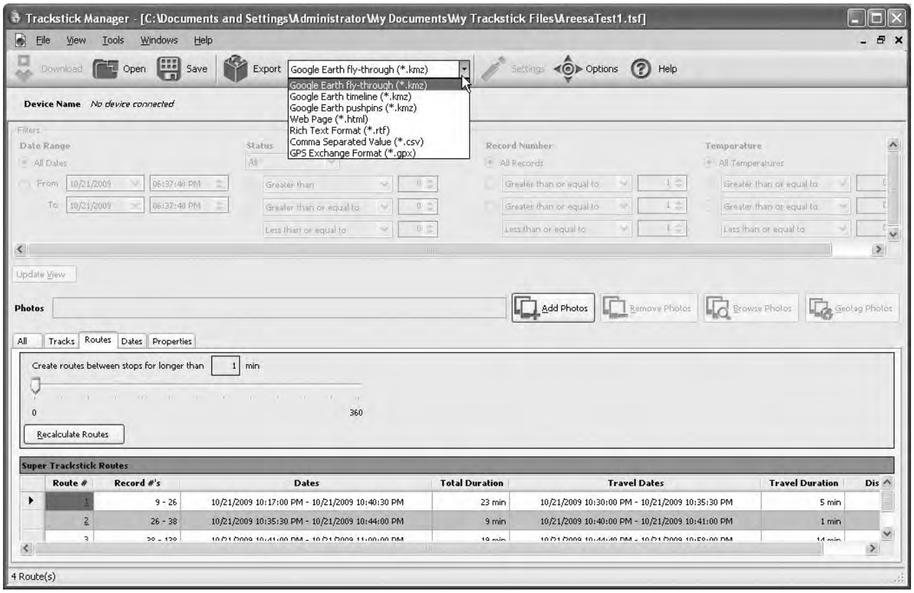



图7-21　导出目标的整个行驶路线

图7-22是从谷歌地图上导出的数据。




图7-22 在谷歌地图上显示目标的移动路线

短短的一节不足以涵盖社会工程人员使用的全部工具，成功的关键在于多练习和研究。知晓什么样的工具能决定审计活动的成败只是成功的基础。作为一名专业的社会工程人员，你必须练习、练习，再练习！了解工具的正确使用方法至关重要。

在网站www.social-engineer.org给出的社会工程人员框架中，我会分析很多提高社会工程人员实践能力的工具。

要想成为成功的社会工程人员，光掌握物理工具还远远不够，因为所有这些工具的应用效果都依赖于其质量及第2章中讨论的全面的信息收集。下一节将讨论世界上最神奇的信息收集工具。

# 7.2　在线信息收集工具

如前所述，信息收集是社会工程的一个关键方面。若在这一点上投入的精力不足，可能会导致社会工程行动的失败。现在，社会工程人员可以通过多种工具来收集、分类以及运用信息。

这些工具完全改变了社会工程人员查看和使用数据的方式。他们将不再局限于使用常规的搜索方式找寻数据，这些工具为他们打开了互联网的资源之门。

## 7.2.1　Maltego

收集和分类信息可能是很多社会工程人员的薄弱环节。如果存在一个工具，它可以同时对一个域名、IP地址，甚至是一个人进行几十种搜索；能提示各项信息的权重，显示信息重要与否；有一个GUI界面，可以用不同颜色表示不同的对象，可以导出利用；最重要的是有免费的版本可用，怎么样？

Maltego就是社会工程人员梦想的工具。这个神奇的工具是由Paterva公司（www.paterva.com）的员工开发的。Maltego有一个免费的社区版本，可以从他们的网站下载，BackTrack4的每一个版本中都集成了Maltego程序。如果想要解除免费版在功能上的限制，如可转换的次数及保存数据，花费大约600美元就可以得到完整的授权。

我参与的一次审计充分证明了Maltego的强大威力。当时我的任务是对一家小公司的网站进行安全审计。目标是入侵该公司CEO的计算机，但他是一个严谨、古板、不常使用网络的人。作为印刷公司的老板，他只关心自己的生意，几乎不使用高科技。显然这项任务极具难度。

我首先打开Maltego。通过该公司的域名，提取所有网站页面和Whois数据库中的电子邮件地址，这是个很好的信息基础。然后我深入查看这位CEO的电子邮件是否在其他网站或链接中使用过。我发现他给当地的一家餐厅写了一些评论，并公开了他的电子邮件地址。同样，他在对另一个州的一家餐厅的评论中也给出了电子邮件地址。从评论中可以发现，他去这个州探亲时去过这家餐厅，评论中甚至提到了他兄弟的名字。使用Maltego做进一步调查，我找到了他父母和兄弟在这一地区的住址。通过对姓氏进行搜索，我找到一些新的链接页面，其中提到了他在那里创业时使用的另一个邮箱，以及他与当地教堂发生了矛盾，而后转到了另一家教堂。随后，我发现他Facebook上链接的一篇博文，其中有他们一家人在观看完最喜欢的球队比赛后的一些照片。下面是我花了不到两小时的时间，用Maltego获得的调查结果。

- 他喜欢的食物；
- 他喜欢的餐厅；
- 他孩子的姓名和年龄；

- 他离婚了；
- 他父母的名字；
- 他兄弟的名字；
- 他长大的地方；
- 他的宗教信仰；
- 他喜爱的球队；
- 他家庭成员的相貌；
- 他过去的生意。

一天后，我给目标发送了一封邮件，里面包含针对当地公司的一个摇奖信息。中奖者可以去他喜爱的餐厅享用一顿免费大餐，同时获得三张扬基队的球赛门票。所有参与的公司必须同意与一名销售代表简单讨论当地的慈善活动。如果该公司同意，其名字就会进入摇奖获选序列，并有机会赢取扬基队的球赛门票。我伪装成“乔”，然后准备了一份与该公司CEO通话的提纲。我的目标是让他接收一个PDF文档，那是我们给他设定的圈套。我打电话的时候，他应该已经收到了我的邮件，我也很容易通过这个话题切入：“是的，他正在等我打电话。”

在与“乔”的通话中，CEO接收并打开了包含详细摇奖信息以及恶意加密文件的邮件，该文件会发起一个反向会话，让我侵入他的系统。

当然，他的屏幕上没有显示任何信息，他只是对Adobe不停地崩溃感到沮丧。我告诉他：“我很遗憾，你无法打开文件。我们会将您的名字列入抽奖名单并且今天会发送一些额外的信息给您。”但在发送邮件之前，我召集了一个报告会，讨论目标是如何被完全入侵的。

这次社会工程活动的成功主要在于使用了Maltego。它能帮助我们以最佳方式收集、组织和分类数据。

Maltego是如何帮助我在这次行动中取得成功的呢？

将Maltego视为一个信息的关系型数据库，能发现互联网上信息之间的联系（在应用中称为实体）。Maltego在后台做了很多工作，如挖掘电子邮件地址、网站、IP地址和域信息。举例来说，点击几下鼠标你就可以通过目标域名自动地搜索到所有相关电子邮件的地址信息。只需在屏幕上简单地增加“电子邮件”转换器，输入想要搜索的电子邮件地址，就可以得到图7-23所示的效果。

#### 使用Maltego的原因

Maltego能自动采集大量信息并为用户实现数据的自动关联，可以为用户节省数小时的搜索时间，并展示信息的关联图。Maltego真正的强大之处在于找到这些数据之间的关系。尽管数据挖掘很有用，但是展示信息之间的关系对社会工程人员更有价值。

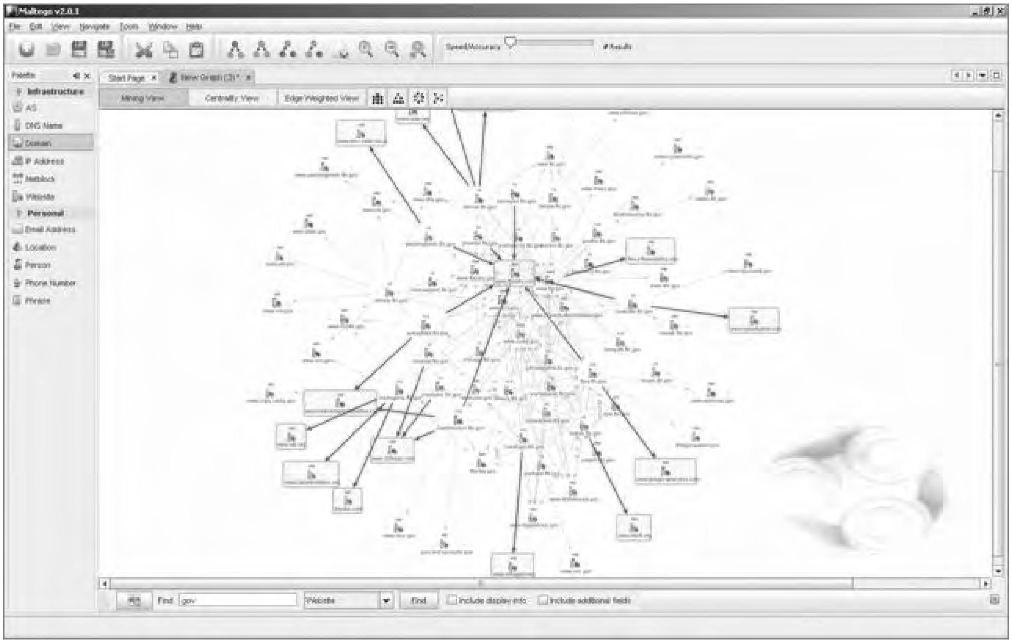


图7-23　Maltego收集的信息展示

我在www.social-engineer.org/se-resources/贴出了一些视频，讲解怎样高效地使用Maltego。前面的案例中Maltego居功至伟，但后续的入侵使用了另外一个强大的工具。

## 7.2.2　社会工程人员工具包

社会工程人员花费了大量时间来完善自身的技能，然而，许多攻击方式需要通过创建附加恶意代码的邮件或PDF文档来实现。

这些事情都可以利用BackTrack中包含的诸多工具来手动完成。起初搭建www.social-engineer.org网站的时候，我曾和好友戴夫·肯尼迪交谈过。戴夫是流行工具FastTrack的开发者，FastTrack使用Python脚本和网页界面能够自动实现渗透测试中的一些最常用的攻击。我对戴夫说，单独为社会工程人员开发一个类似FastTrack的工具是个不错的主意，这个工具让社会工程人员点击几下鼠标就能创建PDF文件、电子邮件及网站等，这样就可将注意力集中到社会工程中的“社会”这部分上来了。

戴夫仔细思考了这个问题，决定创建一些简单的Python脚本，让社会工程人员可以创建附加恶意代码的PDF文件并随邮件发送。于是社会工程人员工具包（Social Engineer Toolkit，SET）就诞生了。在写本书的时候，SET已经被下载了150多万次，而且很快成为社会工程人员审计时配备的标准工具包。本节将介绍SET的主要特点及使用方法。

### 1. 安装

安装步骤十分简单，只需安装Python和Metasploit框架。这两个软件在BackTrack发行版中已经存在，所以不用担心。BackTrack 4甚至已经包含了SET。如果需要从头开始安装，过程也十分简单。依据导航进入安装目录，在控制台窗口上运行如下命令：

```
svn co http://svn.secmaniac.com/social_engineering_toolkit set/
```

执行完命令之后，将得到一个名为set的目录，该目录下包含了所有SET工具。

### 2. 运行SET

运行SET的过程也很简单。只需在set目录下输入`./set`，就会启动初始SET菜单。

请访问www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_%28SET%29，这里有SET菜单的完整展示图，以及对每个菜单选项全面、深入的介绍。接下来介绍SET中两个最常用的功能。

首先讨论鱼叉式网络钓鱼攻击，然后讨论网站克隆攻击。

#### (1) 鱼叉式网络钓鱼

网络钓鱼是一个术语，描述恶意诈骗犯如何通过定向设计的电子邮件“广泛撒网”，吸引人们访问特定的网站、打开恶意文件或者输入个人敏感信息，为以后的攻击做准备。要在今天的互联网世界生存，必须能够检测并防御此类攻击。

社会工程审计人员使用SET可以创建有针对性的电子邮件对客户进行测试，然后记录有多少雇员上当了。这个信息随后可用于培训，以帮助员工识别和避免这些陷阱。

使用SET进行鱼叉式网络钓鱼攻击，选择选项1。选择1后，会看到如下几个选项：

- 执行群发邮件攻击
- 创建一个文件格式负载
- 创建一个社会工程模板

要进行邮件式钓鱼攻击，选择第一个选项。第二个选项用于创建一个恶意的PDF或其他文件，以备作为邮件附件发送。第三个选项用以创建模板，待日后使用。

在SET中发起攻击十分简便，只需选择正确的菜单选项然后点击启动。例如，如果我想发动邮件攻击，向受害者发送伪装成技术报告的恶意PDF文件，我会选择选项1——执行群发邮件攻击。

接下来，我会选择一个攻击向量（选项6），这种攻击对很多版本的Adobe Acrobat Reader软件

都有效——应用了`Adobe util.printf() Buffer Overflow`[1]漏洞。

接下来几个选项会设置攻击的技术问题。点击选项2——Windows Meterpreter Reverse_TCP。使用Metasploit接收反向会话或者受害者电脑的IP和端口，以避免入侵检测系统（IDS）或其他系统的报警。

选择443端口，使数据流看起来好像是加密的SSL数据。SET会创建恶意PDF文件并设置监听功能。

执行上述步骤后，SET会询问是否要更改PDF的文件名，例如改成类似TechnicalSupport.pdf等更加隐蔽的名称，然后输入邮件信息以备收发。最后，SET发出一封看起来很专业的电子邮件，引诱用户打开附件中的PDF文件。受害者收到的邮件如图7-24所示。




图7-24　一封无害的电子邮件与一个简单的附件

邮件发送之后，SET会创建一个网络监听器等待目标打开文件。一旦目标点击了PDF，监听器就会执行恶意代码，让攻击者得以进入受害者的计算机中。

真是惊人（也许有人并不这样认为），所有这一切只需点击六七下鼠标，审计者便可将精力集中在攻击中真正的社会工程方面了。

这是一个破坏性很强的攻击，因为它利用了客户端软件的漏洞，而且在大多数情况下，屏幕上不会出现任何提示。

这只是应用SET可以发动的众多攻击中的一种。

(2) Web攻击

SET也允许审计人员克隆任何网站并在本地运行。这种攻击类型的强大之处在于可以让社会工程人员以多种方式诱骗他人访问克隆网站并从中获利。社会工程人员既可以伪装成更新网站的开发者，也可以仅仅对网址进行细微的修改（填加或删除一个字母），最终诱使他人访问克隆的网站。

① 请参见http://www.nsfocus.net/vulndb/12573。——译者注

一旦有人访问了克隆网站，社会工程人员便可以发动多种不同的攻击，包括信息收集、证书收集和直接入侵等。

要在SET中运行此攻击可从主菜单中选择选项2（网站攻击），选择之后，可以看到以下几个选项：

- Java Applet攻击方法
- Metasploit浏览器的入侵模式
- 证书获取的攻击方式
- 标签绑架攻击方法
- 中间人攻击方式
- 回到前面的菜单

选项1中的Java Applet攻击是一种特别邪恶的攻击。一般情况下，Java Applet攻击会在用户界面上弹出一个Java安全警告，说该网站已被ABC公司签名，并让用户同意这一警告。

进行这种攻击，先选择选项1，然后选择选项2——网站克隆（Site Cloner）。

选择网站克隆的时候，需要输入你想克隆的网站地址。这里可以选择想克隆的任何网站——客户的官方网站、客户供应商网站或者政府网站。正如你所想象的，重点在于选择一个对目标有意义的网站。

在这个练习中，假设是克隆Gmail网站。屏幕上会显示如下信息：

```
SET supports both HTTP and HTTPS
Example: http://www.thisisafakesite.com
Enter the url to clone: http://www.gmail.com
[*] Cloning the website: http://www.gmail.com
[*] This could take a little bit...
[*] Injecting Java Applet attack into the newly cloned website.
[*] Filename obfuscation complete. Payload name is: DAUPMWIAHh7v.exe
[*] Malicious java applet website prepped for deployment
```

上述工作完成之后，SET会询问你想要在自己与被害者之间创造什么类型的连接。要想使用本书讨论的技术，选择Metasploit的反向会话界面，也就是Meterpreter。

SET为负载加密提供了多种选项，这是为了避开反病毒系统的检测。

下一步，SET启动内嵌的网站服务器为克隆网站提供服务，同时启动监听器准备捕获浏览该网站的受害者。

现在只需要社会工程人员构造一封电子邮件或给目标打个电话，让目标访问该假冒的网站。最后，用户会看到如图7-25所示的界面。

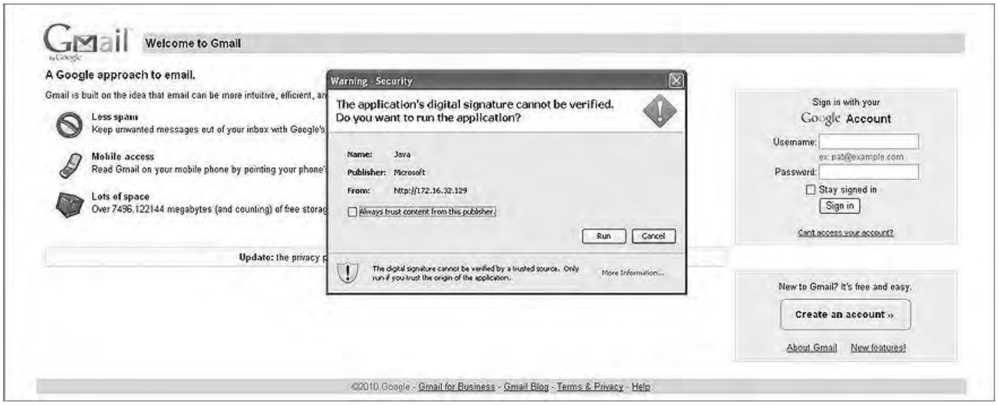


图7-25　谁会不相信微软签名的小程序呢?

最终结果是，一个Java Applet出现在用户面前，告诉他该网站已被微软签名，他需要允许安全证书运行，才能继续访问网站。

只要用户允许了该安全证书，攻击者就可以立刻入侵他的计算机了。

### 3. SET的其他特性

SET是具有实战思维的社会工程人员开发出来的，所以工具集所提供的都是审计过程中常常会用到的攻击方法。

SET在不断更新和发展。例如，最近几个月，除网站克隆和网络钓鱼攻击之外，SET又增加了一些其他的攻击方式，还增加了一个传染性媒体生成器。传染性媒体生成器允许用户创建带恶意文件的DVD、CD或USB，这些传染源可以混杂在目标对象的办公大楼里。当它们被插入计算机时，将触发恶意负载程序的执行，从而开启受害人机器的入侵之门。

SET也能创建简单的负载和相应的监听器。如果社会工程人员想要通过一个提供反向会话功能的EXE可执行程序连接回他的服务器，可以在审计过程中携带一个U盘。如果面前的机器是他想要远程访问的，便可将U盘插入，导入负载文件，然后点击运行。这样可以在目标机器和自己的机器之间建立起一个快速连接。

有一种较新的攻击方式叫Teensy HID攻击。Teensy设备是一个小的可编程电路板，可嵌入键盘、鼠标或其他可插入电脑的电子设备。

SET可对Teensy编程，设置这个小电路板在插入电脑时将执行何种命令。常见的命令包括创建反向会话或监听端口等。

SET的最新特性之一是提供了一个Web界面。这意味着SET会自动启动Web服务器程序，从而更易于应用。图7-26显示了这个网页界面的概貌。




图7-26 SET的新Web界面

SET是一款强大的工具，它能帮助社会工程审计人员测试出公司存在的常见弱点。SET工具的开发者总是善于听取他人的意见，在工具中增添新的应用，使得其不断完善、越来越流行。如果想更深一步了解这个强大的工具，可以登录www.social-engineer.org网站，上面包含每个菜单选项的详细说明。在使用过程中，可以通过www.social-engineer.org和www.secmaniac.com这两个网站不断更新SET。

### 7.2.3 基于电话的工具

社会工程书籍中最早介绍的工具之一就是电话。如今，随着手机、网络语音以及自制电话服务器的出现，社会工程人员使用电话的方式越来越多样。

社会工程人员需要熟练掌握电话的使用技巧以便进行成功的审计，因为人们经常会受到电话销售、推销和广告的骚扰。尽管有一些限制，但作为社会工程的工具，电话还是可以用来在短时间内搞定一家公司的。

在一个人人都有手机的时代，人们会在公共汽车、地铁或者其他公共场合，使用手机接打私人电话或进行深入的交谈，使用手机的方式多种多样。利用手机进行窃听或与目标直接通话，这些攻击方式在过去是不可能实现的。随着市场上智能手机和具有计算机功能的手机日益增多，越来越多的人在手机上储存密码、个人数据和私人资料。这为社会工程人员通过不同场合接触目标、获取数据打开了一扇新的大门。

如果拨号者可以通过某种“方式”提高其可信度，那么每天24小时开机就增加了信息泄露的几率。例如，如果来电显示表明电话是从公司总部打来的，则许多人会毫不犹豫地提供信息。苹果和安卓智能手机都有可供利用的应用程序，可以将来电显示号码篡改成任何号码。利用类似SpoofApp（www.spoofapp.com）的应用程序，社会工程人员能够以较低的成本将拨出的号码伪装成从任何地方打来的电话号码。这一切都将提高伪装的可信度。

社会工程中电话的使用可以分为两个不同的领域：背后的技术和编造的借口。

### 1. 篡改来电显示

来电显示在商务和家用电话中都已成为一项普遍的技术，特别是在当前手机普遍取代固定电话的情况下，来电显示已成为日常生活的一部分。成功的社会工程人员必须意识到这一事实并且知道如何加以利用。

*来电显示篡改*主要是篡改目标的来电显示信息。换句话说，尽管你使用某一号码拨号，但显示在对方屏幕上的却是另一个号码。

利用该技术的一种方法是伪装成在垃圾箱里找到的目标公司的供应商的号码。如果社会工程人员发现ABC公司是目标的计算机技术支持单位，就可以找到该公司的号码，在打电话跟目标预约下午见面时伪装该号码。通过篡改来电显示，你可以伪装成以下机构或个人：

- 远程办公室
- 办公室内部
- 合作伙伴
- 公用事业/服务公司（电话、水、网络及专业灭虫人员等）
- 上司
- 快递公司

到底怎样篡改来电显示呢？下面将讨论一些可供社会工程人员使用的方法和设备。

### 2. SpoofCard

最流行的一种篡改来电显示的方法是使用SpoofCard（www.spoofcard.com/）。使用这种卡，可以假冒随卡提供的800个号码，输入PIN码和希望显示的号码，然后输入想拨打的电话号码就可以了。

SpoofCard的一些新特性也很有用，比如对通话内容进行录音、伪装成男声或女声等。这些特性大大提高了拨号者的伪装能力，社会工程人员可以借此欺骗对方提供其所需要的信息。

从另一方面来说，SpoofCard简单易用，除了电话不需要其他额外的硬件或软件，并且有成千上万的用户证实了它的有效性。SpoofCard唯一不好的一点就是需要付费购买。

### 3. SpoofApp

越来越多的人开始使用苹果、安卓及黑莓等智能手机，这些手机上都有大量的应用可以用来伪造来电显示。SpoofApp将SpoofCard技术实现在了软件包中。

不用真的拨打指定的号码，只需在应用程序中输入想要拨打的电话号码，然后输入想要显示的号码，SpoofApp就会和目标建立连接，而目标电话上显示的就是你输入的想要显示的号码。所有操作只需点击几下按钮即可完成。

### 4. Asterisk

如果有一台多余的计算机和一个VoIP服务，也可以使用Asterisk服务器来篡改来电显示。可以在www.social-engineer.org/wiki/archives/CallerIDspoofing/CallerID-SpoofingWithAsterisk.html页面上找到一些有关这种手段的信息。Asterisk服务器的运行机制与SpoofCard非常相似，只是用于篡改来电显示的服务器不一样。在这种情况下，你使用的是自己的服务器。这一点很有吸引力，因为它提供更多的自由并且不必担心线路中断或时间耗尽。

Asterisk的优点在于免费、安装好后使用简单并具有很大的灵活性，你可以自己控制它。缺点在于不仅需要额外的计算机或虚拟机，还需要知道如何使用Linux，此外还需要一个可用的VoIP服务提供商。

使用Asterisk的最大好处就是，有关呼叫方和被叫方的信息完全由社会工程人员自己控制。个人信息和账号数据不在第三方手中。

### 5. 使用脚本

电话是社会工程人员最喜爱的工具。只需稍稍改变一下伪装，社会工程人员就能在不泄露身份的情况下攻击很多目标。

在使用电话进行社会工程活动的过程中，必须考虑使用脚本。脚本是电话社会工程中必不可少的部分，它能确保所有需要的要素都被涵盖和涉及。不过，脚本不是按部就班的演讲稿。对目标来说，没有什么比对方像背台词般说话更不快的了。

写完脚本之后，应该反复练习，这样才能令你听上去真实、真诚、可信。

这就是信息收集至关重要的原因。信息收集得越全面，脚本编写也就越清晰。我发现掌握目

标的一些兴趣和爱好很有帮助，这样更易于构建共识。

搜集的信息充足有助于你勾勒出攻击计划。在前面讨论的攻击印刷公司CEO案例中，我准备的大纲中包括了要说的关键内容、想要涉及的要点，以及一些提示，如在通话过程中要“清楚地表达”、“不要忘了提及慈善部门”及“放慢语速”等，这让我在打电话时得以集中精力。

使用脚本或大纲（而非照本宣科的草稿）可以让你流利且自然地与对方交流，而且在应对意外状况时也能从容镇定。

电话仍然是社会工程人员十分重要的工具，如果在实际应用中与本书提到的技术和方法相结合，便可以获得成功。

### 7.2.4　密码分析工具

另一组不得不提的工具就是密码（口令）分析工具，它们能帮助你分析目标及其可能使用的口令。在目标信息收集完成之后，下一步就是分析其可能使用的口令和攻击他的方式。社会工程人员可以构建一个潜在的口令列表用于暴力破解。从工具的角度来看，构建可能的口令列表可以加速攻击。本节将介绍几个可用的密码分析工具。

为了完成任务，密码分析工具可能需要持续运行几小时甚至几天。

尽管发出了很多警告，但每年遭到简单攻击的人数仍在不断上升。在网上公开个人信息的人数是惊人的，公开的信息各种各样，关于自己、家庭以及生活琐事等。基于人们在社交媒体上泄露的信息，以及在网络上可以找到的其他信息，凭借接下来讨论的工具，社会工程人员甚者能勾勒出某些人的全部生活。

密码分析卓有成效的原因之一是人们选择密码的方式。实践证实很多人反复使用相同的密码。更糟糕的是很多人使用的密码很容易猜测，而且不需要什么技巧。

最近，BitDefender（一家网络安全公司）的一项研究证实了这一点。BitDefender分析了25万多名用户使用的密码，结果十分惊人：其中75%的用户所使用的邮箱密码和社交媒体账户的密码是相同的。再想想近期有1.71亿Facebook用户的个人信息被人以P2P种子的方式发布到网上，这多么恐怖啊。完整的文章内容参见www.securityweek.com/study-reveals-75-percent-individuals-use-same-password-social-networking-and-email。

2009年，一名昵称为Tonu的黑客做了一项很有趣的研究。通过获取某个流行社交网站近期弃用的URL，他伪造了页面，对试图登录的人进行了一段时间的记录。不过他这样做并没什么恶意。

你可以在www.social-engineer.org/wiki/archives/BlogPosts/MenAndWomenPasswords.html看到研究结果。

其中的一些信息甚至震惊了资深的社会安全专家。在734 000人中，有30 000人使用自己的名字作为密码，有约14 500人使用他们的姓氏作为密码。更惊人的是下面的统计数字，最常使用的8个密码如下表所示。

| 密　码 | 性　别 | 用　户　数 |
|---|---|---|
| 123456 | 男 | 17 601 |
| password | 男 | 4 545 |
| 12345 | 男 | 3 480 |
| 1234 | 男 | 2 911 |
| 123 | 男 | 2 492 |
| 123456789 | 男 | 2 225 |
| 123456 | 女 | 1 885 |
| qwerty | 男 | 1 883 |

17 601位男性使用的密码是123456？真是令人震惊啊。

如果这还不够令人震惊，再看看Tonu公开的统计数据吧：66%以上的用户使用的密码长度为6到8个字符。由于大多数人使用的都是弱口令，通过使用流行的密码破解工具，例如图7-27中展示的“Cain and Abel”，社会工程人员破解这些弱口令并非难事。

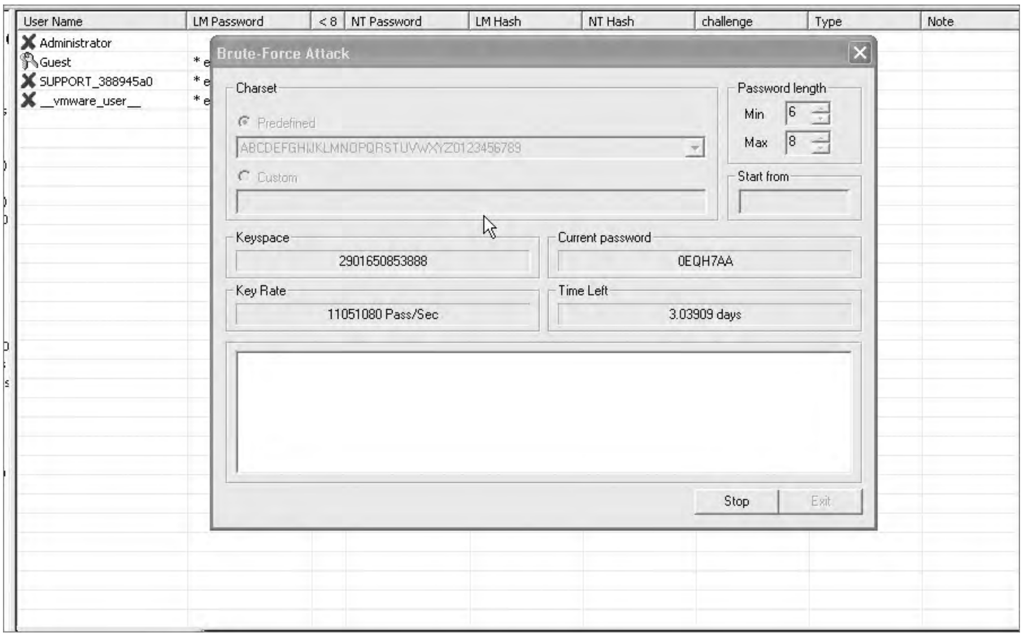



图7-27　破解弱口令只需要3天

请注意剩余时间栏写着3.03909天。对大多数黑客来说，三天就能获得服务器的访问权限算是短的了。难道用三天获取管理员密码算很长吗?

为使这一信息真正切中要害，请看图7-28。如果同一个用户使用14~16个字符的密码，其中包含大小写字母和非字母字符，破解所需要的时间就不是一般地长了。

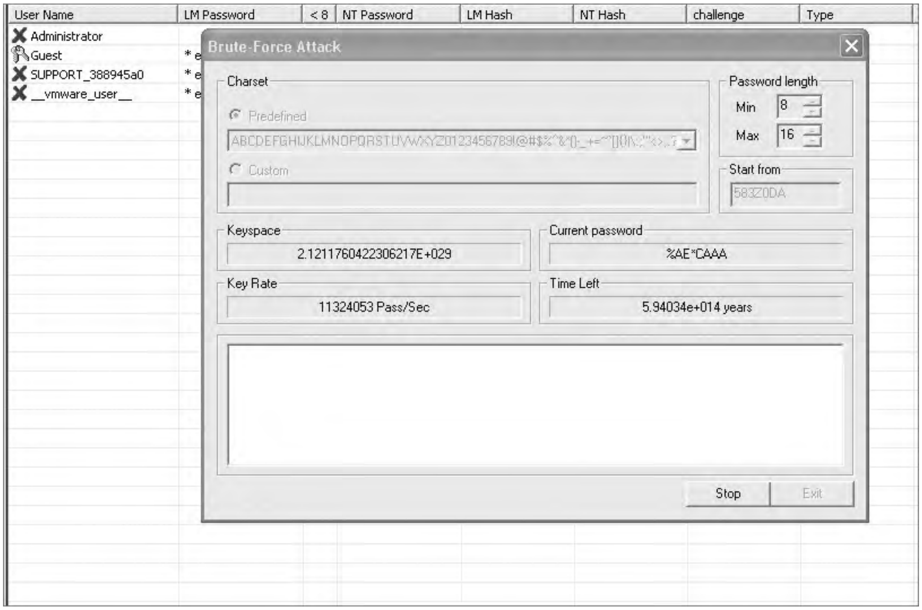



图7-28 剩余时间栏已经增加到几万亿年

超过5万亿年够长吗？仅仅通过将密码长度增加到14位，并使用一些非基本的字符（即*、&、$、%和^），黑客通过暴力破解获得密码就会变得几乎不可能。

由于许多用户不会设置如此复杂的密码，找到他们所使用密码的弱点并不困难。某些工具（下面将会介绍）可以帮助分析用户可能会选择的密码。

### 1. 通用用户密码分析工具

成功社会工程审计的一项重要工作就是对目标对象进行分析。前面给出的Tonu研究案例显示：734 000人中有228 000人以上只使用6位字符的密码，其中超过17 000人的密码是123456，大约4600人使用password作为密码。

通用用户密码分析工具（Common User Password Profiler，CUPP）使得密码分析工作更加简单。

Muris Kurgas，或称为j0rgan，开发了这个神奇的小工具。它是包含在BackTrack渗透测试工具中的一个脚本，也可以通过www.social-engineer.org/cupps.tar.gz下载。

最普遍的认证形式是用户名加密码或口令短语。如果两个值都与本地存储表中的值匹配，用户就可以成功访问。密码的强度就是猜测、使用加密技术或自动化测试库破解密码的难度。

弱口令可能非常短或只使用数字和字母字符，这样就很容易破解。弱口令也很容易被那些对用户进行分析的人猜到，比如生日、昵称、住址、宠物或亲属的名字，或者God、love、money及password等常用单词。

由于大多数用户使用容易猜到的弱口令，因此CUPP是一个完美的分析工具，它可以用于合法的渗透测试和犯罪取证调查。

以下源自BackTrack 4中使用CUPP会话的内容。

```
root@bt4:/pentest/passwords/cupp# ./cupp.py -i
[+] 输入对象信息以生成字典[小写！]
[+] 如果不知道相关的信息，只需输入回车！;)
> 名字：John
> 姓氏：Smith
> 昵称：Johnny
> 生日 (DDMMYYYY; i.e. 04111985)：03031965
> 配偶名字：Sally
> 配偶昵称：Sals
> 配偶生日 (DDMMYYYY; i.e. 04111985)：05011966
> 子女名：Roger
> 子女昵称：Roggie
> 子女生日 (DDMMYYYY; i.e. 04111985)：05042004
> 宠物名：Max
> 公司名：ABC Paper
> 还要加入一些与目标有关的关键词吗？ Y/[N]：Y
> 请输入每个词，以逗号分隔 [i.e. hacker, juice, black]：christian,polish,sales person
> 需要在每个词的尾部加入特殊字符吗？ Y/[N]：N
> 要在每个词的尾部添加一些随机数吗？ Y/[N]n
> 黑话模式？(i.e. leet = 1337) Y/[N]：Y
[+] 现在生成字典……
[+] 排序并移除重复字符……
[+] 字典保存到文件中，共生成13 672个密码
[+] 现在你可以使用了，祝好运！
```

请注意，根据所提供的资料最后创建了包含13 672个密码的字典文件。此类工具的作用在于减少了社会工程人员猜测密码的工作量。

## 2. CeWL

据其开发者描述，CeWL是一个Ruby应用程序，它可以通过给定的URL进行指定深度的搜索，并可扩展到外部链接，最终生成一个可用于密码破解的字典文件，John the Ripper等密码破解工具可以使用这个字典进行密码破解。有关CeWL的更多资料请参见www.digininja.org/projects/cewl.php。下面看一下在BackTrack 4中使用的情况。

```
root@bt:/pentest/passwords/cewl# ruby cewl.rb
```

```
 --help cewl 3.0 Robin Wood (dninja@gmail.com)
(www.digininja.org)
Usage: cewl [OPTION] ... URL --help, -h: show help --depth x, -d x: depth to spider to,
default 2 --min_word_length, -m: minimum word length, default 3 --offsite, -o: let the
spider visit other sites --write, -w file: write the output to the file --ua, -u user-
agent: useragent to send --no-words, -n: don't output the wordlist --meta, -a file:
include meta data, optional output file --email, -e file: include email addresses,
optional output file --meta-temp-dir directory: the temporary directory,default /tmp -v:
verbose URL: The site to spider.

root@bt:/pentest/passwords/cewl# ./cewl.rb -d 1 -w pass.txt http://www.targetcompany.
com/about.php
root@bt:/pentest/passwords/cewl# cat passwords.txt |wc -l 430
root@bt:/pentest/passwords/cewl#
```

这是针对某个目标公司网站使用CeWL的案例，从其网站的一个网页中产生了430个可能的密码。

CUPP和CeWL只是用来帮助分析和生成潜在密码的两个工具。运用这些工具做一个有趣的实验，输入自己的信息，看看你的密码是否能够被生成。这样会使你清醒地认识到密码安全的重要性。

## 7.3　小结

工具是社会工程的一个重要方面，但工具本身不足以成就社会工程人员。仅有工具是没有用的，掌握工具的功能并实际运用才是重点。

本章的核心主题在于熟能生巧。无论是使用电话、基于软件的工具、网络还是其他间谍工具，练习使用才是成功的基石。例如，在社会工程活动中使用电话时，可以篡改来电显示甚至变换说话的声音。然而，如果在使用这些神奇的技术时，你的声音听起来过于生硬、紧张、不安或者准备不足、言之无物的话，那么你所期望的成功就会落空，并且很有可能让一切变得不可信。这项原则在应用伪装技术时同样非常适用。你要伪装的那个人如何谈吐？他会说什么？他会怎么说？他掌握了什么样的知识？ 他会询问什么样的信息？

不管社会工程人员使用软件工具、硬件工具，还是两者都用，都应该花时间去学习每个工具的详细功能，因为工具的每个特征都会影响审计工作的成败。

工具能节省大量的审计时间，并可弥补审计人员潜在的不足。这一点在第8章的案例分析中体现得尤为明显。

第 8 章

# 案例研究：剖析社会工程人员

安全之本在于教育。

——马蒂·阿哈罗尼

本书涵盖了如何成为一名杰出社会工程人员的各个方面。若将这些内容运用于实践，社会工程人员会成为难以对付的人。

上学时，学生通过学习历史来了解什么可为、什么不可为。历史是一个很伟大的工具，能告诉我们过去哪些行为成功了以及为何会成功，也能为我们指明前进的方向及方式。

社会工程的历史也不例外，纵观其整个发展史，充满了欺诈和偷窃行为，也有很多人为对抗恶势力鞠躬尽瘁，奉献了一生。

要探讨专业社会工程攻击的方方面面是十分困难的，因为这种行为要么是非法的，要么由于委托合同的限制不能公开讨论。幸运的是，凯文·米特尼克（Kevin Mitnick，世界著名的社会工程人员及计算机安全专家）共享了许多有趣的故事供我们了解。本书从他的著作《欺骗的艺术》中选取了一部分故事。

本章我从米特尼克的书中选取了两个最著名的案例，简单重述了凯文的做法，分析了其中涉及社会工程方面的内容，并且讨论了大家能从中学到什么。

分析完那两个案例之以后，我会分析自己的两个案例，以表明信息获取之简单，以及利用信息入侵整个公司又是何等地轻而易举。最后，我会公开两个不能透露来源的“最高机密”，但你会发现从这些故事中可以学到很多东西。我的目的是告诉你，即使是一丁点信息，若落入技术高超的社会工程人员手中，也会造成极大的破坏性。同时，你也可以看到社会工程人员如何从之前

的成败中吸取经验教训，以提高自己的技能。

下面让我们来看看第一个案例。

## 8.1　米特尼克案例 1：攻击 DMV

凯文·米特尼克是世界上最著名的社会工程人员之一。他曾进行过一些举世闻名的、胆大妄为的攻击，下面列出的案例尤其如此。

通过驾照来获取他人的信息是很方便的。通过目标的驾照号，社会工程人员可以获取各种个人信息。然而，天下没有免费的午餐，社会工程或者私家侦探必须耗费一番精力后才能获得这些信息，并利用其对目标进行攻击。

凯文·米特尼克在《欺骗的艺术》一书中讲述了一个叫“反向之刺”的故事。下面几个小节将简要介绍这个故事的背景并展开分析。

### 8.1.1　目标

在讲述的最精彩的案例之中，米特尼克描述了“艾瑞克”如何利用非公开的机动车辆管理局（DMV）和警察系统获取人们的驾照号。艾瑞克经常需要收集目标对象的驾照信息，而且在这方面很有一套，但是他也担心频繁使用电话社会工程的方法会引起DMV的警觉，甚至会让警察找上门来。

他需要设计出另一种访问DMV网络的方法，而且根据对DMV运作方式的了解，他也知道怎样着手去做。他的目的是双重的，即不仅是DMV，甚至警方也会协助他（当然是在不知情的状况下）获取信息。

### 8.1.2　故事

艾瑞克知道DMV可以向保险公司、私家侦探和其他特定团体提供机密信息，它们只可以访问对其开放的特定类型的数据。

保险公司和私家侦探可以获取的信息不同，而司法部门可以得到一切信息。艾瑞克的目标是获得所有的信息。

#### 1. 获取非公开的DMV电话号码

艾瑞克所使用的步骤和方法证实了他非比寻常的社会工程技巧。首先，他通过查询台询问DMV总部的电话号码。当然，他得到的是面向公众的号码，而他真正想获得的是更深入的内部信息。

接着，他致电当地县治安官办公室，请求转接呼叫中心，该呼叫中心是协调各司法部门之间信息传递的办公室。在打电话给呼叫中心时，他向工作人员询问司法部门呼叫DMV总部时所使用的专用号码。

在对方不了解来电者身份的情况下，这个举动很可能会以失败告终，但他采取的是下面的做法。

“请问您是？”对方问道。

他必须快速地回答：“我是艾尔。我拨打的电话是503-555-5753。”

他所做的就是随机报一个区号相同、基本号码相同、最后4位数字纯属编造的号码，然后戛然而止。该司法办公室的工作人员可能做出了以下假设：

- 来电者是内部人员，并且知道这个非公开的中心号码；
- 来电者似乎知道DMV所有的号码。

由于工作人员坚信上述两种假设，艾瑞克顺利得到了想要的号码。但是，艾瑞克想要的并非只是一个号码，他想要掌控握尽可能多的信息。

要想实现这一目标需要进行更深入的攻击——通过多种不同方法，多层次、多角度的攻击，而这种攻击是很惊人的。

### 2. 入侵州电话系统

艾瑞克使用获取的号码致电DMV，并告诉接线员他是北电网络有限公司（Nortel）[①]的工作人员，因为工作涉及DMS-100（一种广泛使用的交换机），所以需要同DMV的技术人员交流。

当与技术人员通话时，艾瑞克又自称是得克萨斯州北电技术服务中心的工作人员，并且解释说他正在更新所有的交换机，更新过程会通过远程进行，只需要对方提供交换机的拨入号码，他就可以从技术服务中心直接进行更新。

这个故事似乎完全可信，所以技术人员照办了，给了艾瑞克所有需要的信息。利用这些信息，他现在能够直接拨入一个州电话交换系统。

### 3. 获取密码

下一个障碍是整个攻击行动中的关键一环——获取密码。DMV所使用的北电交换机有密码保护。根据以往的经验，艾瑞克知道北电交换机有一个默认的用户账户——NTAS。随后他几次拨入系统，尝试遇到过的标准密码：

- NTAS——失败

① 加拿大著名的电信设备供应商，可参见百度百科的文章http://baike.baidu.com/view/238246.htm。——译者注

- Account name——失败
- helper——失败
- patch——失败
- update——成功

哇噢，真的吗？密码是update。现在他获得了整个交换机和连接线路的控制权限。通过查询电话线路的走向，他很快找到通向同一个部门的19条电话线路。

在检查交换机的内部设置后，他发现交换机的工作机制是先搜索19条线路，直到发现其中一个状态为不忙时，就建立连接。他挑选了18号线路，输入标准转发代码，为这条线路增加了呼叫转移控制。

艾瑞克买了一个预付费的便宜手机，以便于随意丢弃。他将这个号码设置为18号线的自动转接号。这样，只要DMV有17条线路都处于忙碌状态，第18次呼叫就不会进入DMV，而是直接呼叫艾瑞克的移动电话。

启动后不久，大约在第二天上午8点，手机就响了。每次，电话那头都有一位警官来询问某人的信息。艾瑞克可能在家里、餐馆、车里等地方接到警察拨来的电话，不管是在哪里，他都假装成DMV的接线员。

让我啼笑皆非的是下面这个电话。

手机响起，艾瑞克说道："DMV，请问有什么可以帮你的？"

"我是安德鲁·科尔侦探。"

"你好，侦探先生，请问今天有什么可以帮你的吗？"

"我需要查探一下驾照号为005602789的人。"

"好的，让我调一下他的记录。"在假装操作电脑的同时，艾瑞克会开始询问："科尔侦探，您的警局在？"

"杰斐逊县。"

艾瑞克还会接着问如下问题："您的请求代码是？""您的驾照号码是？""您的生日是？"

来电者会将个人信息全盘奉上，艾瑞克只是假装核对，然后假装确认来电者查询的信息。他会假装查阅名字和其他信息，接着说："对不起，我的电脑刚才又死机了。侦探先生，我的电脑这周总是不停地出问题。您能重新打进来找另一位工作人员帮忙吗？"

对侦探来说，这肯定很叫人恼火，但从道理上也说得过去。在这个过程中，艾瑞克已经掌握了那位侦探的身份。这些信息可以用在很多地方，但最重要的是可以随时从DMV获取信息。

在从DMV收集几小时的信息后，艾瑞克再次拨入DMV的交换机，取消转接功能。现在他已经拥有足够多的信息了。

在攻击之后的几个月里，艾瑞克还是能轻易地拨入，打开交换机的呼叫转移功能，继续收集警官的用户信息，然后取消呼叫转移，用警察的身份去获取有效驾照的个人信息，然后出卖给私家侦探或者其他不会在意这些信息来源的人。

### 8.1.3 社会工程框架的运用

这个故事里，凯文总结了一些促使艾瑞克成功的做法和表现，例如在和警察谈话时要保持淡定以及迂回地处理不熟悉的问题。

你也可以找出艾瑞克所用的社会工程框架及使用方法。

举个例子，任何成功的社会工程审计或攻击的第一步都是信息收集。从这个例子中你可以发现，艾瑞克一定是事先做足了功课才开始攻击的。他对电话系统、DMV的运行方式以及有待渗入的流程颇为熟悉。我不清楚这个攻击发生在多久以前，但是现在有了网络，这种攻击就更加简便了。网络是信息收集的金矿。几年前有人想出了一种攻击Tranax ATM取款机的方法，几个星期之后在互联网上就可以找到实现这种攻击的详细手册了。

同样，如本书之前提到的，选择与你的工作或曾经的身份相似的身份来伪装，能增加成功的几率， 因为伪装得越“逼真”，就越有利于收集信息并攻破目标。显然艾瑞克谙熟此道。

也许你还记得，框架的下一步就是诱导，即能通过精心构思的问题来套取信息或获得访问权限。艾瑞克套取信息的能力超群。在与警察通话的过程中，他通过诱导策略证实了自己就是所伪装的角色并且非常了解自己的“工作”。他知道行话以及必要的例行问题。事实上，不问那些问题反而会比问更可能引起警觉。这就是优秀的诱导策略的威力所在。

艾瑞克早就知道他需要套取特定的电话号码去发起攻击。他没有解释自己为什么需要这一信息，而是使用了第3章中提到的假设性问题，简单地说：“我得知道答案，告诉我就好了。”这是强力诱导的另一个例子，你可以细致地分析他使用的方法，并从中学到很多。

大部分优秀的攻击同时也包括大量的伪装，这个例子也不例外。艾瑞克在这次攻击中设计了一些伪装，他必须多次转换身份才能达到目的。他伪装的执法部门的工作人员给人留下了深刻的印象（他做得非常好），但请牢记，这种行为在美国是严重的违法行为。你能从艾瑞克的社会工程过程和使用的方法中学到很多知识，但是在应用时必须小心谨慎。即使在付费的社会工程审计活动中，假冒执法部门的工作人员也是违法的。

要了解当地的法律，这是经验教训，否则就不要害怕被逮捕。尽管实际上是非法的，你仍可以通过分析艾瑞克在攻击中的表现学到很多。他总是很镇定。当伪装成DMV工作人员时，他能

够使用诱导技术来证明自己的身份。伪装成警察时，他的行为、声音和措词都支撑着他的伪装。对很多人来说，转换身份是极具难度的，所以在进行“直播”表演前最好多加练习。

艾瑞克的伪装技术十分精湛，特别体现在伪装成DMV的工作人员和回应警察打来电话的时候。很多情况下，他可能会露出马脚，但最终似乎掌控得很好。

社会工程中常运用到许多心理学方面的技能，比如眼神和微表情，本例中没有用到，因为这次攻击主要是通过电话完成的。但是艾瑞克确实应用了框架中的一些技术，例如关系构建、神经语言程序学以及思维模式。

艾瑞克似乎是个建立关系的天才。他风度翩翩、平易近人，处理意外情况时泰然自若，能自信地伪装各种角色。他的声音和谈吐让电话那头的人完全有理由信任他。

艾瑞克所使用的提问和交谈策略令人印象深刻，他甚至将这些技巧应用在了谙熟此道的执法人员身上。他成功地运用这些策略并在对方不知不觉中获取了他想要的所有信息。

艾瑞克还很好地掌握并运用了影响策略，在攻击中最明显的表现之一就是他要求警察致电另一位DMV工作人员。这很可能惹恼对方，但是这个策略的成功之处在于艾瑞克之前已经“给”了对方一些信息，也就是他“核实”了对方需要的信息，只不过就在他要为对方提供最后一部分信息的紧要关头，“计算机”挂了。

通过运用一些影响力的规则，艾瑞克轻松地让对方听从了他的意见。

与艾瑞克的伪装密不可分的是他成功运用了框架。回忆一下，框架是令自己和自己的故事可信，从而使目标的思维与你的思维一致。这是伪装的关键之一，能使你的伪装更加完美，并使目标对你的话深信不疑。艾瑞克的伪装技巧精湛可信，但是真正让目标信任他的是他使用的框架。他的框架取决于谈话的对象。有时候他必须让电话那头的办公人员为其提供呼叫中心的号码，有时候他需要成为业务技能娴熟的DMV工作人员。

艾瑞克利用框架使自己高度可信，他假定自己会获得所询问的信息，在应对过程中没有慌乱，并且自信地提出每一个问题，让对方“感觉”作出回答是他的义务。所有这些表现使对方落入他的设计，相信他的伪装，并自然地作出了回应。

正如你所看到的，通过分析艾瑞克的社会工程攻击你能学到很多东西。你能够猜想出，艾瑞克要么练习过所有这些攻击方法，要么进行过多次模拟和演练，以便熟悉如何处理攻击中使用的那些内部系统。

虽然艾瑞克的方法奏效了，但我还想补充一些预防措施。举例如下。

- 处理DMV电话时，我会先确保自己是在“办公室”里再进行呼叫转移。我会设置一个有些背景噪音的办公环境，并准备好记录所有信息所需的设备，以避免我在记录时被服务生或朋友打断而露陷。

- 尽管对反追踪来说，使用一次性手机是个好主意，但还有一种技术可以应用，即利用谷歌语音服务（Google Voice）或Skype号码转拨。我不信任手机信号，因为掉线、信号微弱且不稳定可能瞬间就会导致攻击失败。

除了这两项，他的攻击中基本没什么需要改进的了。艾瑞克充分运用了社会工程框架中的各项技巧，确保了攻击的成功。

## 8.2　米特尼克案例 2：攻击美国社会保障局

米特尼克的书中曾提到一个名叫基思·卡特的人（Keith Carter），他是一位不那么可敬的私家侦探，受雇调查一位男士，该男士即将离婚，但对妻子隐瞒了存款情况。那位妻子曾资助丈夫创业，如今当初的小生意已发展成为一家价值数百万美元的公司。

离婚是在所难免的，但女方的律师需要找到男方“隐瞒的财产”。这个攻击十分有趣，因为和第一个案例一样，这个案例中也将使用一些不法方式收集信息。

### 8.2.1　目标

目标是为了查明丈夫乔·约翰逊的资产情况，但那不是社会工程攻击的目标。为了获取乔的信息，私家侦探基思必须对美国社会保障局（SSA）进行攻击。

在社会工程审计活动中，经常会攻击社会保障局。本节介绍了基思为实现目标所使用的方法，但可以说攻击社会保障局不啻于跳崖。随着故事的展开，你会发现这个特殊的攻击有多么地危险。

### 8.2.2　故事

乔·约翰逊与一个非常有钱的女人结婚后，从她那里得到了好几万美元的投资去实现自己的创业梦想，后来他创立了一家价值数百万美元的公司。

渐渐地，他们的婚姻出现了裂痕，最终双方决定离婚。在办理离婚手续期间，约翰逊夫人“得知”丈夫隐瞒了其真实的财产情况，想要逃过财产分配。

她雇用了基思，一个不那么光明磊落的私家侦探，一个为了达到目的不在乎手段是否违法的人。

在着手分析案情时，基思认定社会保障局就是他的绝佳突破口。他认为，如果能得到乔的财产记录，从中发现不一致的地方，就能给他致命的一击。他想伪装成乔，这样就能够随意地打电话给乔的银行、投资公司以及境外账户查询信息。为此，他还需要一些详细的信息，这促使他决定攻击社会保障局。

基思开始基本的信息收集。他上网找到一本指南，其中描述了SSA的内部系统、内部专业术语以及行话。在了解了系统并将行话背得滚瓜烂熟之后，他给当地社保办公室的公众热线打了一个电话。电话连线后，他要求接通理赔办公室，对话如下。

“你好，我是格雷戈里·亚当斯，329区办公室的。我想找一位理赔调解员，他正在处理一个以6363结尾的账号，具体账号我已经传真过去了。”

“噢，他在3部，号码是……”

真的吗？那么简单？哇噢。几分钟的时间他就获得了一般公众难以获得的内部办公电话。接下来进入较难的部分。

他必须致电3部，改变他的伪装，套取有关乔的有价值的信息。周四早晨，基思的计划似乎已经做好了，他拿起电话拨通了3部的号码。

“这里是3部，我是王梅林（May Linn Wang）。”

“王小姐，我是亚瑟·埃洛丹，从监察长办公室打来的。我可以称您为‘梅’（May）吗？”

“请叫我‘梅林’。”她回答道。

“好的，是这样的，梅林。我们有个新人现在还没有电脑，现在他有些要紧的事，所以用了我的。我要抗议，我们可是美国政府部门，他们竟然说没有足够的预算为新人配置电脑。现在我的上司认为我怠慢工作，不想听我的任何借口，你懂吗？”

“我明白你的意思。”

“你能帮我快速地在MCS上查一些信息吗？”他问道。MCS是查询纳税者信息的计算机系统名称。

“当然，你需要查什么？”

“首先，请帮我按照字母顺序查找约瑟夫·约翰逊（Joseph Johnson），生日是1969年7月4日。”（字母序查找是通过纳税人的姓名进行计算机搜索的一种方式，之后再以出生日期进一步定位。）

“你想知道什么？”

“他的账户号码是多少？”基思问道（即乔的社会保障号）。

她直接就读了出来。

“我还需要你对那个账号做数字查找。”（数字查找类似于字母序查找，只不过是通过数字而不是字母查找。）这需要她报出纳税人的基本数据，梅林回复了纳税人的出生地、母亲结婚前的姓氏和父亲的名字。基思耐心地听着，梅林还给出了乔社会保障号发放的日期和发放单位。

基思接下来请求查询乔的具体收入。

“请问要哪一年的？”

“2001年。”

梅林说：“数额为190 286美元，付款人是约翰逊微技术公司。”

“还有其他收入吗？”

“没有了。”

“谢谢，”基思说，“你人真好。”

基思打算以后每次需要获取信息却“没有电脑可用”时都打电话给她，这是社会工程人员钟爱的一套把戏，因为建立了联系之后他们下次还能和同一个人通话，免去了每次找寻新目标的麻烦。

“下个星期不行。”她告诉他，因为她要去肯塔基州参加姐姐的婚礼。其他时间，她会尽力而为。

此时任务貌似已经完成了。基思获取了他想要的所有基本信息，接下来的任务就简单了，只需再给银行和境外账户打一通电话，获取相关的信息即可。

这真是一场顺利实施并令人惊叹的攻击。

### 8.2.3 社会工程框架的运用

SSA攻击可能会让你瞠目结舌。从这个应用了社会工程框架的特殊攻击中，你能获益颇丰。

基思首先进行了信息收集。可能你已经听烦了，但是获取信息是所有优秀社会工程人员攻击的核心所在，掌握的信息越多就越有利。

基思首先在网上找到了令人震惊的内部资料，而且现在竟然还能在https://secure.ssa.gov/apps10/poms.nsf/上找到。

这个链接直接指向社会保障局操作程序的在线手册。手册中包含了缩写词、行话、操作指南以及SSA工作人员可以向执法部门提供的信息。掌握了这些信息，基思知道该说什么、问什么、怎样让自己看起来像是那么回事儿，以及什么样的信息是不能问的。

尽管链接提供了大量的信息，但他决定伪装成监察长办公室的工作人员，致电SSA以深入搜集信息。他从外部突围，通过本地公众热线获取了内部号码，随后又伪装成内部工作人员。

基思在此过程中完美地转换了好几次伪装。通过SSA在线手册的帮助，他获得了很多信息从而顺利提问。这本手册简直就是诱导者的梦想之书。通过运用恰当的词句，他听上去真像那么回

事。他还通过构建共识和框架使伪装惟妙惟肖。构建共识并非易事，但是基思在这方面做得很好，证明他之前做了充分的练习。他运用了很多影响策略以使目标对象感觉合情合理，从而放松了警惕。例如，他把义务和将心比心巧妙地结合了起来。当讲述自己没有好工具且无法获得管理层的支持时，他让梅林觉得有义务去帮助他。

他也使用了关键词和短语来博取同情，同时又表明自己是政府部门的工作人员，比如“我的上司对我很不满意”，这句话暗示他处于麻烦之中，而SSA的工作人员梅林可以帮助他。人们在道德层面有一种帮助有需要的人的责任感。很少有人会对求助者置之不理，梅林也是如此，她不仅感到有义务施以援手，甚至还告诉了基思她的个人行程。

最终，基思运用了社会工程框架中一系列不需当面使用的重要技巧。

政府系统是由人管理运行的，这令它们难以抵抗本例中所使用的攻击方法。这里并非建议使用自动化或计算机系统代替人的操作，而是仅仅指出一个事实，即很多系统过于依赖超负荷工作、低薪、处于高压状态的人员来操作，结果造成操纵这些人并非难事。

老实说，要对这次特殊的攻击进行改进很难，因为我一般不会进行这样的攻击，而且基思在应用社会工程框架的过程中已经做得相当杰出了。

许多人都习惯于被虐待和辱骂，些许善意就能令他们不遗余力地伸出援手。正如米特尼克在《欺骗的艺术》一书中声称的，这次特殊的攻击表明依赖于人进行操作的系统很容易被攻击。

## 8.3　海德纳吉案例 1：自负的 CEO

我与一位自负的CEO的交锋经历还是比较有趣的，因为那位CEO认为自己绝对不可能被任何社会工程渗透，理由有两个：第一，生活中他不常使用科技类产品；第二，他天资聪颖，完全能够抵抗他所谓的“愚蠢的游戏”。

在内部安全小组了解上述信息之后，他们决定让我将该CEO作为安全审计的目标。他们知道，如果他不能通过审计，那么此后的安全整改工作审批会更容易些，这有益于保障公司的整体安全。

### 8.3.1　目标

目标是美国一家规模较大的印刷公司，该公司拥有一些工艺专利和供应商，而且一些竞争者在打它们的主意。IT部和安全部门认为公司存在一些薄弱点，并说服CEO有必要进行一次安全审计。在与我搭档的一次通话中，该CEO傲慢地说，他知道攻击他简直是无稽之谈，因为他将会用生命保守这些秘密。即使是他的某些核心雇员也不知道所有的细节。

作为社会工程审计师，我的工作是渗透公司、获取公司某一台服务器的访问权限，并拿到其

中存储的专利信息。就像CEO在电话里提到的，困难之处在于服务器的密码都存储在他的电脑里，没有他的允许，即使是安全部门的职员也无法接触他的电脑。

### 8.3.2 故事

很明显，不管采用什么方式，都必须通过CEO这一关。这的确是一个挑战，因为CEO已经全副武装，就等着被渗透了。我依照惯例由信息收集开始，通过网络资源和其他工具（比如Maltego）调查该公司。通过这种方式我获得了很多信息，比如服务器位置、IP地址、邮箱地址、电话号码、公司地址、邮件服务器、员工的名字和头衔等。

当然，我把这些信息制成文档以备之后使用。邮箱地址的结构十分重要，在调查他们的网站时，我发现其邮箱地址的结构是“名字.姓氏@公司名.com”。我没能找到CEO的邮箱地址，但网站上的许多文章都提到了他的名字和头衔（姑且称他为Charles Jones，即查尔斯·琼斯）。这些是普通的、不了解详情的社会工程人员都可以获取的信息。

利用“名字.姓氏@公司名.com”的格式，我尝试发了一封邮件给他，但是没能成功。这令我非常失望，因为我确定通过邮件方式能得到许多具体的信息。

我决定尝试一下Charles的昵称Chuck（恰克），于是试了试“chuck.jones@公司名.com”，竟然成功了！我获得了经过验证的邮件地址。现在我要验证一下这个邮箱是属于CEO的，而不是与他同名的某个家伙。

我花了更多的时间通过谷歌和Maltego尽可能地搜集更多的信息。Maltego有一个强大的转换器插件功能，可以像搜索引擎一样搜索域名范围内的任何文件。

我对公司域名范围内的文件进行转换，大量的文件映入我的眼帘。Maltego通过转换插件不断地提供文件名，许多文件包含元数据，其中包括了日期、创建者和其他的细节信息。通过运行Maltego的元数据转换功能，我发现其中很多文件都是由“Chuck Jones”创建的，文件中的许多内容都暗示他就是CEO。

这正是我想证实的，但在浏览的过程中，一个特殊的文件引起了我的注意——InvoiceApril.xls。这是当地一家银行开具的关于某个营销项目的发票，他参与了该项目，其中有银行的名称、日期以及资金数额，但是缺少具体的项目名称信息。

于是我快速查询了银行网站，但是6个月之前的项目已经无法显示了。我该怎么做呢？

我决定给银行市场部的人打一个电话。

“你好，我是某某公司的汤姆。我在整理账本，发现其中夹了一张4月份的面额为3500美元的赞助发票。项目名称没有写，你能告诉我这是什么活动的发票吗？”

“当然可以，汤姆，”伴随着键盘的敲击声她说，“我查到这是银行儿童癌症基金会发起的年度活动，贵公司是银牌赞助商。”

“非常感谢。我是新来的，非常感谢您的帮助。再见。”

我想到了一种可用的攻击方式，但还需要更多的调查研究，然后周密地计划一次电话通话。

我在网站上找到一些关于筹款活动的文章，以及许多公司为癌症治疗研究出资赞助的报道。另外，我对CEO做了更深入的调查并收获良多，我发现了他父母的名字、他姊妹的名字、他放在Facebook上的孩子的照片、他住在父母附近时去过的教堂、他对喜爱的餐厅的评价、他喜欢的球队、他大儿子喜欢的球队、他读的大学及他孩子上的学校等。

我想知道为什么公司要捐款给儿童癌症基金会。尽管利用他人的感情是许多恶意社会工程人员的所为，但我意识到可能自己也不得不这么做，因为我想知道是否是因为他某个儿子是癌症患者他才加入基金会的。我打了个电话给公司市场部的经理。

“你好，我是XYZ的汤姆。受本镇第一国家银行的委托，负责联系4月份儿童癌症基金会的出席者，能耽误您一点时间做个反馈调查吗？”

“当然可以。”市场经理苏说道。

“苏，我看到你们是4月份活动的银牌赞助商。你觉得就宣传结果而言这笔赞助费花得值得吗？”

“嗯，这是我们每年都会做的，在当地会有不少报道。如果网站上能多展示些银牌赞助商的信息就更好了。”

“好的，我记下来了。每年？是的，我看到你们每年都会这么做。个人想了解一下，有那么多基金会，为什么选择了我们？”

“据我所知，恰克总是特别关注这个。他是CEO，我想大概是他家里有人得了癌症吧。”

“噢，我很抱歉。请问是他的孩子吗？”

“不是的，我想可能是他的侄子或表妹吧。我也不是很肯定。”

“好的，十分感谢你们的捐款和支持。”

我又提了一些问题，再次表示感谢，然后结束了通话。

我得到了想要的信息——不是他的孩子患有癌症。我知道这不会阻止一个恶意的社会工程人员进行攻击，但我还是很好奇。在得到这些信息之后，我开始计划入侵攻击。

我知道CEO来自纽约，喜欢一家名叫多明戈的餐厅，并且经常带着孩子看大都会的比赛，然后去多明戈餐厅吃饭。

他给餐厅写了评价，并且列举了最喜欢的三道菜。我从他的Facebook中了解到，目前他还是和父母住得很近，而且经常过去探望。

我计划伪装成癌症研究资金的募集人员，宣称在为三州地区筹款，捐款的人将有机会抽奖，奖品是两张大都会比赛的门票和一张餐厅的优惠券，可从三家餐厅中任选一家，多明戈餐厅就是其中之一。

我会假装自己来自纽约地区，但是工作时间不长，以防他提到一些我不知道的事情。

我的最终目标是让他接收一个包含恶意代码的PDF文件，该代码能够让我反向入侵他的计算机。但如果他没有使用能让我成功入侵的Adobe软件版本，我会接着说服他下载一个zip文件，并执行其中带有恶意文件的EXE安装程序。

为了成功伪装，我针对通话内容进行了一番练习，测试了PDF和EXE文件，并且打开谷歌地图找到了多明戈餐厅的位置以备通话中可能谈到。准备好用来接收受害者反馈信息的电脑后，一切工作准备就绪。

大约下午4点，我拨通了电话，因为通过公司网站我发现该公司周五下午4:30下班。由于以前与他洽谈审计事宜的不是我，而是我的搭档，所以CEO听不出我的声音。

“你好，请问查尔斯·琼斯先生在吗？”

“请稍等。”电话那头的声音有些疲惫，并且该人马上为我转接。

“你好，我是恰克。”

“你好，琼斯先生，我是美国癌症研究会的托尼。我们正在进行一项年度资金募集活动，筹得的资金将用于支持癌症研究，目前不管男女老幼都在饱受癌症的折磨。”

“请叫我恰克。”他打断了我。

这是一个好兆头，因为他并没有以现在很忙等借口挂断我的电话，并且在对话中融入了个人色彩。我继续说道：“恰克，谢谢你。我们正在进行一项募款活动，联系的是原先捐过款的单位，这次是50~150美元的小额捐款。为此，我们为捐款的好心人设置了包含两项大奖的抽奖机会，抽中的话会赢得两张纽约大都会比赛的门票以及一顿免费的双人晚餐，有三家餐厅可供选择。本次抽奖一共会产生5位幸运者。”

“大都会比赛，真的？”

“是的。也许你对大都会的比赛不感兴趣，但餐厅还是非常棒的。”

“不，不，我喜欢大都会，我会那么问是因为我太高兴了。”

“好的，请考虑一下。你不仅能帮助癌症研究，还有机会观看精彩的比赛，而且还能在莫顿、巴塞尔和多明戈三家餐厅中选择一家免费就餐。”

“多明戈！真的？我喜欢这家餐厅。”

“哈，那太好了。你知道我前几天第一次去那，那儿的蘑菇鸡肉真是棒极了！”这是他第三大爱的菜。

“哦，那不算什么，你应该尝尝法式菠萝，那是那家餐厅最棒的菜，我每次去都点它。”

“我周末会再去那，一定要试试。谢谢你的推荐。现在时间也不早了，我不是来要钱的，也不能从电话里拿走钱。我会发一个PDF文件给你，你可以看看，如果感兴趣的话，填一下表格，然后随支票一起发过来就可以了。”

“好啊，发过来吧。”

“好的，还有几个问题，你的邮箱地址是？”

“chuck.jones@公司名.com。”

“如果可以的话，请打开PDF阅读器，单击‘帮助’菜单上的‘关于’，然后告诉我版本号。”

“稍等，版本是8.04。”

“很好，我可不想发一份你打不开的文件。稍等不要挂，我现在就发过去。好了，发过去了。”

“好的，谢谢。真希望我是幸运儿，我太喜欢那家餐厅了。”

“我知道，那儿的菜的确不错。在挂电话之前，你能检查一下邮箱，看看邮件是否收到了吗？”

“好的，我5分钟后就要注销了，不过还能查看。是的，收到了。”当听到双击的声音，我开始检查运行于我的BackTrack电脑上的恶意负载侦听程序Meterpreter（见第7章），它正在响应。我屏住呼吸（这部分从来不会无聊），砰地一声命令行界面出现了。Meterpreter脚本的属主信息改变了，类似于Explorer.exe。

恰克嚷道：“啊，我黑屏了，不能动了。”

“真的吗？真是奇怪了。让我检查一下。”我真正查看的是我是否能访问他的硬盘，并且立刻上传反向命令行，这在他关机重启后还能运行。我说：“很抱歉，我不知道怎么会这样。你能再等我几分钟吗？”

“好的，我去洗洗咖啡杯，离开会儿，不挂电话。”

“好的，谢谢。”这段时间足够我确保下次还能进入他的计算机系统了。很快，他回来了。

“我回来了。”

“恰克，这真让人尴尬，但我不清楚发生了什么。我不想耽误你的时间，要不你先回去，我重新做一个PDF文件再发邮件给你。我们周一再联系。”

“好，没问题。周末愉快！”

“你也是，恰克。”

挂断电话后，令我吃惊又惊喜的是，他的电脑没有关机，并且处于活动状态。是的，他将一切保存在了安全的硬盘中，而且只有他有权访问，不过全都保存在了Word中。我立即开始下载那些Word文档，几个小时后我访问了服务器，打印出他想保护的所有内部工作流程。

我在周一早上联络了他，但不是以基金募集者托尼的身份，而是以安全咨询专家的身份，而且携带了包含他的“秘密”和密码的打印文件，还有与他及其员工的通话录音。

成功攻击后，与客户第一次会面时，他们往往大为震惊，并且会宣称我们使用了不道德的策略，利用人性弱点实现入侵。当我们解释说恶意分子会使用同样的战术时，他们由愤怒变为恐惧，最后会表示理解。

### 8.3.3 社会工程框架的运用

与之前的案例类似，我们将本案例与社会工程学框架结合，分析该攻击的精彩之处，以及哪些部分还有待改进。

像往常一样，信息搜集是社会工程的关键，在这个案例中也是一样。信息搜集有很多渠道——网站、Maltego及电话等，这些是成功攻击的基础。信息不足将会导致悲惨的失败。

恰当而丰富的信息关系重大，甚至是我不需要的信息，类似他去的教堂、他父母和兄弟姊妹的名字，都在信息收集的范围之中。这些都是以防万一，有备无患，但是邮件地址的惯用格式以及用Maltego找到的服务器上的文件却是非常宝贵的关键信息，正是这些信息为我打开了入侵该公司的大门。

就像第2章提到的，将搜集到的信息分门别类地保存到BasKet或Dradis中，方便随时使用信息也很重要。相反，包含一大堆信息的文本文件会很难利用。信息整理与信息搜集是同等重要的。

像坏人一样思考（尝试挖掘并利用目标的弱点和欲望）并非工作的关键，但是如果专业的审计人员想要保护他的客户，他将会竭尽全力地去证实其客户有多么脆弱。搜集的信息越多，就越容易发现漏洞。这就是通向成功的道路。

增强伪装的真实性和设计话题有助于攻击的成功。你必须提出有力的问题并抓住关键点来吸引目标的注意。通过搜集大量的信息，我能提出有效的问题并制定一个涉及关键词和神经语言程

序学用语的框架，这会大大提高战术影响力的威力，确保攻击的成功。

我不得不经常更换伪装，以员工的身份打电话给公司的供应商，再以供应商的身份打电话给内部员工以获得更多的信息。我必须仔细地准备每个身份，进入角色，这样才能在实战中应对自如。这当然需要很多时间的谋划，以确保每个伪装都合理、自然。

熟能生巧。在发起攻击前我和搭档反复练习。我必须确保PDF文件正常工作，攻击方法合理，还必须具备足够的知识，让所有目标都相信我。

人们常常不理解练习的重要性。练习能使我们弄明白什么策略可行、什么策略不可行，并且确保计划顺利开展和实施，甚至在出现意外的情况下也能从容应对。

之后，我发现做一些小小的改进会让这次攻击变得更有效率。首先，仅仅依靠恶意PDF文件是存在风险的，我会建立一个小网站，模拟真实的癌症研究网站，并把PDF文件上传上去。网站和PDF文件都可以包含恶意代码。这样，成功的几率就增加了一倍，其中一个失败了还能有个后备。

另一个更大的风险是CEO离开办公室后还开着电脑。如果他不这么做，我就必须等到下周一才能继续尝试访问。我应该先发给他一份包含恶意代码的PDF文件，待该文件攻击他的电脑后，再发一份“真实的PDF文件”让他阅读。这样他就会在电脑前停留足够长的时间，也好让我有时间利用漏洞进行攻击。

在这次审计中，我花费了大约一个星期的时间去调查、搜集、整理信息以及练习，最后才发起攻击。一个星期的时间，该公司的机密就可能落入了竞争对手或者更高的出价者手中。多读几遍这个故事，体会其中使用的微妙的方法以及对话方式。书面形式很难体现声音、音调和对话节奏，你要试着想象，如果自己处于这些对话场景，将用什么方式处理。

## 8.4　海德纳吉案例 2：主题乐园丑闻

对我来说，主题乐园丑闻是个很有趣的案例，因为它涉及一些现场测试。在这个案例中我运用了本书中提到的许多社会工程技巧，这是一场对理论的实战检验。

第二个原因是其本身的商业性质和骗局成功的可能性。如果成功了，社会工程人员可以获取上千个信用卡账号。

### 8.4.1　目标

本次攻击的目标是检测某主题乐园票务系统的安全性。在登记顾客购票信息时，每个计算机终端都会与后台服务器端的客户信息和金额记录建立连接。主题乐园想看看攻击者能否运用恶意的方式使工作人员采取某种行动从而造成危害。

我的目的不是找工作人员的麻烦，而是为了证明工作人员进行票务登记的计算机被入侵时会带来什么安全危害。此外，我不会采用黑客技术入侵计算机，而是要应用社会工程学方法。

如果这样的入侵发生了，后果会怎么样呢？会泄露什么样的数据？哪些服务器会遭受入侵？但他们并不想考虑得如此深入，只想看看第一阶段，即社会工程入侵是否真能实现。

为了弄清社会工程入侵是否可能，我必须先弄清乐园的售票操作流程，以及工作人员在终端上将会做什么、不会做什么，更重要的是，他们有权做什么、无权做什么。

## 8.4.2 故事

就像前面提到的，这项工作的目的并不复杂，即我只需弄清楚售票窗口的工作人员是否会允许“顾客”让他做一件明显不被允许的事。在开始具体筹划之前，我必须先了解他们的业务内容。

我浏览了乐园的网站，利用Maltego和谷歌调查了有关该乐园的报道和其他信息。我还做了现场调查，亲自去了乐园，体验在售票窗口买票的过程。在这个过程中，我与工作人员进行了简单的交谈，并且留意他们的布局、电脑结点以及“办公室”的其他方面。

这个“办公室”令我有了眉目。在对话中，我提到自己来自一个非常有名的小城镇。她问我是什么地方，我告诉了她，然后她作出了常规的反应：“那地方在哪？”

“你这能上网吗？”

“能啊。”

“哦，你会喜欢上那里的，打开一下谷歌地图，输入邮编11111，然后转换成卫星视图模式。看那个小镇是多么地小呀！”

“我的上帝啊，真是太小了！我以前从来没听过这个地方。”

在这么短的时间里，我掌握了如下信息：

- 售票员工作场所的布局
- 工作人员是怎样售票的
- 计算机是连外网的

我再次登录乐园的网站，开始寻找新的突破口。我需要找到入侵他们计算机系统的方法。我的伪装（一名带着家人去乐园游玩的父亲）很合理。

我设计的故事情节是这样的：一开始家人和我并没有计划去乐园游玩，但是在酒店上网时看到了乐园的优惠信息，于是去大厅打算购买门票，但是那的价格要比网上贵很多。

当我们再次确认价格时，发现优惠价仅适用于在线支付，于是我们在线付了钱，之后才突然

意识到，门票需要打印出来才能被检票器扫描。我试着在酒店打印，可惜他们的打印机坏了。我已经付了钱，害怕钱就这么浪费了，于是把它们转换成了PDF格式并且发送到自己的邮箱里。这个故事听上去很合理，不是吗？我需要做的就是开始着手我的小阴谋。我先打了一个电话。

“你好，是XYZ主题乐园总办事处吗？”

“是的，有什么需要帮忙的吗？”

我需要同内部人员取得联系，向他们提问并且得到我想要的答案。连线采购部门后，我找到了正确的目标。我说：“你好，我是SecuriSoft公司的保罗。我们正在为新的软件产品做免费测试，它能阅读甚至打印PDF文件。我发给你一个免费下载的地址，请试用一下好吗？”

“可以，但是我不确定我们对此会不会感兴趣，但你可以发一些资料给我。”

“太好了，我能问一下你现在使用的Adobe阅读器是什么版本的吗？”

“我想还是第8版的。”

“好的，今天我就发一些合适的资料给你。”

知道版本信息后，我要做的就是创建一个嵌入反向会话的恶意PDF文件（一旦打开，我就能访问他们的计算机），把它取名为Receipt.pdf，然后发送给自己。

第二天，我带着家人开始了一项社会工程行动。家人站在一边等着，我走上前热情地与售票员攀谈了起来。

“嗨！你好吗……缇娜？”我看着她的胸牌说道。

“你好，需要我帮什么忙吗？”她微笑着询问我。

“是这样的，我和家人决定本周末进行一次短途旅行，现在我们住在这附近的希尔顿酒店。”我指着不远处的家人回答道，“我女儿看到了你们主题乐园的广告，于是求着我们带她来。我们答应她了，然后在网站上看到了优惠的门票……”

“噢，是的，我们只在网上提供优惠，现在十分受欢迎。我能看一下你们的门票吗？”

“呃，这就是我想请你帮忙的地方，我不想得到‘年度最烂老爸奖’。”我女儿正在紧张地笑呢。我解释道：“缇娜，我和妻子看到网上的价格便宜15%，就在酒店的电脑上购买了门票，但是付完钱后，酒店的打印机坏了，无法将票打印出来，于是我把它保存为PDF文件，并发送到了我的邮箱。”

“我知道这是个奇怪的要求，不过你可以登录我的邮箱，然后帮我打印一下吗？”这个邮箱地址很普通，包含一些名为“孩子的照片”、“爸妈结婚纪念日”之类的邮件。

可以看出她在做激烈的思想斗争，我不敢肯定她的沉默是否对我有利，或者我可以再推动一下。我说：“我知道这个要求比较怪，但是我的宝贝女儿真的很想去，而且我不想对她说‘不’。”我再次指向女儿，她的表情很配合，流露出可爱而又焦虑的神请。

“好的，我要怎么做呢？”

“先登录gmail.com，然后登录我的邮箱Paul1234@gmail.com，密码是B-E-S-M-A-R-T。”（我知道这个密码很糟糕[①]，但是紧要关头的一点警告也无伤大雅。）

几分钟过后，缇娜双击了PDF文件，然后电脑黑屏了。“你在开玩笑吗？或者我哪里操作错了吗？哇，现在我肯定要得‘年度最烂老爸奖’了。”

“你知道怎么回事吗，先生？我感到十分抱歉，要不然你购买成人票，我让孩子免费进去。”

“哦，你真是太慷慨了。”我微笑着给了她50美元，谢谢她的所有帮助，然后让她退出了我的邮箱。就当我女儿因进入乐园而感到喜悦的同时，主题乐园的系统也被入侵了。

几分钟过后，搭档发短信告诉我，他已经“进入”并且“收集”了报告所需的数据。几个小时的娱乐过后，我们离开了乐园，回去完成了周一会议所使用的报告。

### 8.4.3 社会工程框架的运用

正如本案例中所展示的，信息收集不仅可基于网络，还可以亲自到现场收集。这个案例中的大量信息就是我去现场亲自采集的。找到他们所使用的计算机系统、了解目标对特定问题的反应及查出票务系统的运作方式是本次信息收集的主要内容。

这次攻击中最重要的一点是，好的伪装不仅仅是编造一个故事、装扮一下造型、假冒一下口音，而是可以毫不费力地“设身处地”。

在这个场景中，我能自如地把握父亲的口吻、动作和谈吐，因为我就是一个父亲。我对获得“年度最烂老爸奖”的担心是真实的而不是假装的，我的感情是真挚的，所以会让目标觉得我是真心的。这一切让我的言行更加可信。

当然，有一个可爱的孩子站在远处，用渴望的眼神望着售票员，以及酒店打印机坏掉的情节也十分可信。在第2章中曾提到过，有时社会工程人员需要提升伪装能力，或者至少是个说谎能手，但我相信实际上不止这么简单。

从专业角度来看，伪装需要创建一个现实的、能操纵目标感情和行为的角色。人们通常不会被一些简单的谎言所蒙骗。一名社会工程人员必须“就是”那个伪装的角色，所以选择与你生活

① 密码BESMART的含义是“聪明些”，有点警告的含义。——译者注

贴近的角色是一个不错的主意。

“免费试用PDF软件”这个借口存在很大的漏洞。这个借口本身是没问题的，但是可能会被立即拒绝从而影响下一步的攻击。还有一个侥幸就是售票员所使用的PDF阅读器版本和公司所使用的一样，没有升级，这才让我有机会入侵。

通常，我认为利用人类固有的惰性就是一场赌博，但是在这个案例中我成功了。有时候最好的办法就是相信自己提出的要求是理所应当的。这能让你感到自信，让目标相信你的言行是正当合理的。

正如我在第5章中提到的，使用类似“我真的需要你的帮助……”这样句子，是一个非常好的技巧。乐于助人是人类的天性，特别是当别人开口请求时。

即使是完全陌生的人，在面对请求时也会竭尽全力地给予帮助，就像此案例中从别人的电子邮箱中打开一个未知文件。帮助一个“可怜的父亲”，让他可爱的女儿进入乐园，这样一个请求却导致公司系统被入侵。

一旦入侵成功，存储所有客户的信用卡信息的程序就会成为攻击者的猎物。轻松收集一些数据，就可能让乐园蒙受巨额损失、面临诉讼以及陷入困窘。

## 8.5　最高机密案例 1：不可能的使命

每当我和同事参与或者听到一些给力的情节和故事时，都希望它能够被拍成电影。但出于安全因素的考虑，我们不能泄露内情，所以写和说都是不可以的。出于这些原因，我不能提及真实的参与者以及故事中泄露的信息。下面是一个有关一位化名为“提姆”的社会工程人员的故事。

提姆的目标是入侵一台存储着至关重要信息的服务器，如果这些信息被泄漏了，将导致灾难性的后果。这台服务器的合法所有者是一家知名的公司，他们对它设有重重防护。与该公司签订获取信息的合约时，提姆清楚地认识到自己必须用尽全力，这项工作可以说是对他社会工程技能的挑战。

### 8.5.1　目标

这次攻击的目标是获取一家知名企业的某些商业机密，这些机密绝不能泄露给竞争对手。这些秘密被安全地存储在服务器上，没有任何外部访问通道，信息只能从内网访问。

提姆与该公司签订协议，帮助该公司测试其安全性，防止“恶意人员”入侵并窃取信息。协议是在公司外面签订的，协议内容之前已经通过电话和邮件的方式谈妥了。

## 8.5.2　故事

提姆面临一个巨大的挑战。按照社会工程的步骤，第一步是信息收集。提姆不知道攻击中会使用到什么样的信息，所以他开始了冗杂的收集过程，内容包括邮件布局、报价申请表、所有能找到的员工姓名、他们参与的社交网站、他们发表的文章、他们参加的俱乐部以及他们的服务供应商信息。

他计划去翻一下公司的垃圾箱，却发现垃圾桶周围的安全戒备森严。许多垃圾箱甚至还与外部隔离，所以除非他能翻墙而入，不然连垃圾箱的标志都看不到。查出处理废品的部门后，他决定按照他绝妙的计划给公司打一个电话。

"你好，我是TMZ垃圾处理公司的保罗。我们是本地区新成立的一家垃圾处理公司，已经有一些大公司选择了我们的服务。我是负责贵公司所在区域的销售人员。我能发送一份服务报价单给你吗？"

"可以，我们对现在合作的对象很满意，不过你可以发一个报价来看看。"

"好的，我能快速地问你几个问题吗？"

"当然。"

"你们有多少垃圾箱？"提姆问道。在询问了他们是否有特殊的针对纸张、U盘和硬盘的垃圾箱之后，他最后又问了几个问题。

"你们通常哪天叫人来收废品？"

"我们每周叫人来收两次，第一区是星期三，第二区是星期四。"

"谢谢。我准备一下报价，然后明天下午发给你。你的邮箱地址是什么？"

"你可以发送到我的个人邮箱：christie.smith@company.com。"

现在他们开始了友好的闲谈，不知不觉中，他们说笑着寒暄了起来。

"太感谢你了。嘿，挂电话之前，你能告诉我你们现在是和哪家公司合作吗？我想做一份与他们的比较报价。"

"恩，你知道的……"她犹豫了，但还是说了，"好吧，我们现在的合作伙伴是'废物管家；公司。"

"谢谢你，克里斯蒂。我相信你一定会对我们的报价满意的。我们稍后再联系。"

有了这些信息，提姆打开废物管家公司的网站，将他们的公司标志保存为JPG文件。然后他

访问了在线衬衫打印网站，72小时后，他就收到了一件印有该标志的衬衫。因为知道垃圾将在周三周四被回收，所以他决定周二晚上行动。

接着他又给安全部门打了个电话。

“你好，我是‘废物管家’公司的约翰，你们的废品回收服务商。克里斯蒂・史密斯的办公室来电说你们有一个垃圾箱损坏了。我知道收废品的日子是周三，所以我想明天晚上去看一看。如果有损坏的情况，我们会随车装一个新的去。我周二晚上过去方便吗？”

“好的，让我查查。可以，乔明天在。你就停在保安亭旁边，他会给你张出入证的。”

“多谢。”

第二天提姆穿着“公司”的制服，手拿一块记事板出现了。他的伪装非常到位，因为他清楚日期还有内部工作人员的名字。现在，作为一名服务公司的员工，他走到保安亭前。

“乔，我是垃圾清理公司的约翰，昨天来过电话。”

门卫打断说：“是的，我看到你的名字了。”他给了提姆一张出入证和一份地图，告诉他怎样走到放置垃圾箱的地方。“需要有人陪你去吗？”

“不用了，我很熟悉。”

提姆随即驱车前往垃圾箱的放置点。

完美的伪装和一张出入证为他提供了足够的时间进行信息挖掘。他知道第二区存放的是非食品类垃圾，所以就先从那里开始。

没过多久，他就找到了几块硬盘、几个U盘、几张DVD光盘和一些装满纸的袋子，将它们全部放入卡车中。过了一小时左右，他告别门卫，并且对他们说问题解决了，然后开车离开了。回到办公室后，提姆开始深入搜索这堆“垃圾”中的信息，竟然有了意想不到的收获。

公司经常将不要的硬盘和U盘完全毁坏后再丢弃，他们会擦除上面的数据再送到专门的回收部门。但是，总是有些员工不严格遵守回收处理程序，把不能用的U盘或者无法启动的硬盘随手扔掉。他们没有意识到的是，有些软件可以在不启动硬盘或介质的情况下导出其中的数据，甚至在某些介质已经被格式化的情况下，数据也是可以恢复的。

废品中有一袋文件，内容看上去像是属于办公室的。掏空这个袋子后，提姆找到了一些没被粉碎的纸张。他开始阅读，其中有一份是关于IT服务的合同标书，这项服务工作几天后就会开始。这张纸看上去像是擦拭过溢出的咖啡，然后被丢弃的。

这是一个重大发现，但是还需要进一步调查。DVD光盘都是空白的或者不能读，但惊喜的是他在U盘中找到了一些文件。从这些信息中他发现了CFO的名字及其私人专线，以及其他一些重

要的人事信息。

他收集到的信息具有很大的价值，但是我们需要关注的是他的下一步行动。由于掌握了与IT服务公司签约的信息以及服务的内容，提姆故意在第二天午餐时间给合同联系人打了个电话，期望他出去吃午餐了。

“你好，请问塞巴斯蒂安在吗？”

“他不在，出去吃午饭了。请问我能帮你吗？”

“我是XYZ技术公司的保罗。我想确认一下我们团队是否可以明晚到达，然后开始项目。”

“是的，请记住不要影响我们的正常工作，所以尽量不要在下午5:30之前到这里。”

“好的，先生，我知道了。明天见。”

提姆知道第二天他不能与其他“同事”一起到场，但是如果时间安排得好的话，他就不会被IT服务公司和目标公司的人逮个正着。在黑暗的停车场内等候了许久，他看见IT服务公司的人来了。大约30分钟后，他走到门口，解释说他和刚才进去的人是一起的，只不过刚刚返回车中去取一些文件。他获准进入了，现在他可以自由地进入办公区域了。

他还需要侦察一番，他认为最好的方式就是以内部工作人员的身份接近IT服务公司的人。徘徊了一会儿，终于听到有人在交谈，并且从一个人的穿着看出他是IT服务团队的一员。

由于从U盘的文件内容中得知了一些高层管理人员的姓名，并且从合同中获知了合同联系人的姓名，他上前说道：“你好，我是保罗，CFO施瓦茨先生的手下。有人给你解释过prod23生产服务器的事吗？”提姆从收集到的信息中获悉了服务器的名字，而且知道这正是那台需要他入侵的服务器。

“是的，我们知道那台服务器是禁止接触的。CFO向我们说明了它的加密情况和重要性。不用担心。”

几分钟交谈过后，提姆掌握了一些有价值的信息：

- IT服务人员不能接触服务器；
- 服务器采用了整盘加密；
- 内部IT技术人员“炫耀”说，只能通过管理员携带的U盘上的密钥文件访问。

提姆知道，最后一点会增加他任务的难度，因为管理员不在场，他现在不能访问服务器。另外，服务器的物理安全措施也非常坚固，看上去很难闯入。他十分明确一点，就是管理员可以访问服务器，所以决定从这一点下手。

首先，他来到管理员的第一间办公室，但是门是锁着的。他继续检查第二间，然后是第三间。

第三间办公室的门关着但没有关严，他稍稍一推，就进去了。

为了防止自己被当场抓获，他拉上窗帘关上了灯。他随身携带的社会工程工具套装中装有许多软件和衣物，进行此类攻击时他经常携带的一个工具是Linux启动U盘，比如BackTrack。在BackTrack中预装了一个免费的开源虚拟机工具Virtual Box软件。

他将U盘插入管理员计算机后面的USB端口，启动进入BackTrack。之后，通过SSH与自己的计算机建立连接，创建一个监听程序，然后通过管理员的计算机建立反向会话，继而在BackTrack中启动一个键盘记录程序（记录计算机上键盘敲击的所有信息），通过SSH将这些记录发送到自己的计算机上。

接着他给出了致命的一击。他打开Virtual Box软件，新建一个Windows虚拟机，使用本地硬盘作为启动盘，加载虚拟机。换言之就是，它加载了管理员的账户信息和操作系统。他将虚拟机的登录画面切换成全屏模式，隐藏所有的工具栏，将Virtual Box中现有的退出热键修改成一个特别长的组合键。这是为了防止用户误打误撞而暴露他们被攻击的事实。

通过后端U盘将本地硬盘载入虚拟机的方法，随时都存在被抓的风险，但是这个方法奏效的话，他就能得到管理员每次敲击键盘的记录，而且此人计算机上开放的反向连接使得他可以访问所有内容。即使链接不是在虚拟机中，通过管理员敲击键盘的记录，他还是可以使用受害者的用户名和密码进入到虚拟机中。

提姆在办公室里还做了另外几件事情，例如在另一台电脑上也建立了连接，以提供远程访问入口。他还通过手机SIM卡设置了一个远程监听装置，他可以使用任何一部电话拨打这个号码，监听该装置约6米范围内的对话。

几小时后，提姆离开目标公司回到自己的办公室。他很兴奋地检查这些装置是否能正常运行，但是他还有一些想法要实施。

第二天一大早，他确定远程连接还开着，于是拨通了监听装置，听了听人们早晨进入办公室的情况。正如他所期望的，计算机的第一条记录来了，捕获了管理员的用户名和密码。

大约一小时后，提姆看到不断有记录传进来。他知道如果此时有所行动的话，可能会让连接暴露，所以他只能等着。大约12:15左右，记录传送停止了，他猜想管理员一定是去吃午饭了。他立刻检查了反向会话，利用捕获到的服务器密码从管理员的机器上创建了一条到服务器再到自己机器上的通道。

建立完通道后，提姆在下午1点之前发疯似地尽可能复制数据。那时他没有看到任何键盘记录，无意中他听见监听器中有人问："你知道这会还要开多久吗？"

得知管理员可能在开会，他发起了一个更大的传输任务。大约30分钟后，他发现了一些活动迹象，所以暂停了信息收集，想等晚点再看看。他可不想引起管理员的任何怀疑和警惕，因为文

件传输连接可能会减慢其上网的速度。他开始筛选从服务器上抓取的数据，收获颇丰。

工作还没有结束。那天晚上他传输了大量的数据，可以说是尽其所能，然后再次来到了目标公司，像之前一样通过社会工程方法进去了。他来到管理员办公室，发现门是锁住的拉不开，于是用推刀（见第7章）把门打开了。

进去之后，他先关闭虚拟机，然后拔下U盘重启计算机，依老路离开管理员办公室。他收好监听器，确保没留下什么痕迹。

离开大楼，回到自己的办公室后，他整理了一天的收获。当然，去参加报告会时，他带了一叠打印文件和一个装满数据的硬盘。房间里的每个人都目瞪口呆。

### 8.5.3 社会工程框架的运用

这个故事让我们受益良多。这是一个杰出社会工程人员的例子。这个过程可以总结概况为练习、准备，当然还有信息收集。可以想象，他使用的所有技巧，从推刀的使用到建立通道，再到有效的伪装与信息收集，都是经过不断练习才得以熟练应用的。

对于信息收集的重要性，这里就不再赘述了。我知道大家对此已耳熟能详，但是必须指出的是，如果提姆没有做适当的信息收集，那么此次行动必败无疑。

通过打电话和现场勘查的充足准备，以及恰当硬件设备的选取，提姆的这次行动取得了成功。通过分析这次攻击行动，你可以看到一些社会工程基本原则的实际运用。

提姆是一个信息收集大师，利用网站资源牵出了各种有价值的信息，在打电话时运用了专业的诱导技巧，并且在与目标面对面时运用了杰出的说服技巧。这些技能使得他收集信息的水平远远超出了那些未经专门训练的黑客。

信息收集奠定了提姆伪装与提问的基础。

垃圾箱翻查计划十分精妙。在没有工作服和预约的情况下，他可能进入吗？当然。可是，他的方式到底是多么地有说服力呢？他没有令任何一个和他打交道的人产生怀疑，而且他们都毫不犹豫地按工作流程行事。如果一个人在接触你时丝毫没有引起你的防备和警惕，那他的伪装就堪称完美。提姆做到了，并且可以在垃圾区自由活动。

最精彩的部分是他进入大楼之后发生的事。出问题的几率极大，任何不当的行为都可能让他被逮个正着。他可以进入服务器房间，取走数据然后离开，可能都不会有人阻止他。但是如果采用这种方式就意味着公司不会知道他们的机密是如何被窃取的，也不会意识到他们的计算机曾被入侵过。

提姆冒着极大的风险在管理员的电脑上运行了一个虚拟机。这个特殊策略失败的可能性太高

了。如果有人重启了计算机或者电脑突然宕机，又或者管理员碰巧误按了那个巨长的组合键，都会毁了整个攻击行动，并提醒公司他们的计算机已经被入侵了。

我可能会采取不同的、风险较小的方法，使用定制的EXE程序在他的计算机与我的服务器之间建立反向通道，通过修改计算机的启动脚本，使这个EXE程序不会被杀毒软件检测到，这样失败的可能性更低，但是提姆的方法属于十分有个性的社会工程攻击。

从这次特殊的攻击行动中，我们学到的可能不止一点，但最重要的一点是，“不要轻易相信任何人”这句古老的黑客格言。如果有人打电话说克里斯汀批准了某人检查垃圾箱，但她没有亲自告诉你或者备忘录中也没有，则需打电话向她询问。晚上要关闭电脑，确保它在没有密码的情况下无法通过U盘启动。

当然，这些额外的预防措施意味着更多的工作量和更长的加载时间。是否值得去做得由机器中储存的数据的重要性决定。在这个案例中，这些数据足以使这家公司倒闭，所以保护措施应该做到极致。虽然公司在服务器周围采取了许多先进的预防措施，例如硬盘加密、摄像头及生物锁等，却没能保护那些能够访问最重要的数据的计算机，这可能将会导致整个公司的终结。

## 8.6　最高机密案例 2：对黑客的社会工程

思维不拘一格且快速敏捷是社会工程人员的标准技能，所以对专业的社会工程人员来说，陷入困境的情况很少见。如果在没有事先警告的情况下，让一名渗透测试人员进行社会工程，又会出现怎样的情况呢？

下一个案例就将讲述这一罕见的情况。这是一个非常好的例子，将证明平时多练习社会工程技能在紧急情况下会大有裨益。

### 8.6.1　目标

“约翰”需要为一个大客户进行一次标准的网络渗透测试。审计大纲中没有任何关于社会工程和现场的工作，这可谓是一次没有任何刺激的渗透测试。然而，他还是很乐意为客户找出网络中的安全漏洞。

在这项审计中，一开始确实没发生什么惊心动魄的事。他按照常规路数扫描并记录数据，测试可能被入侵的端口和服务。

就在一天的工作快结束的时候，他通过Metasploit扫描找到一个开放的VNC服务器，通过这个服务器可以控制网络中的其他计算机。这是个不错的发现，因为全部网络是被限制访问的，所以这种简单进入的方式特别受欢迎。

约翰正在记录所发现的开放VNC会话，突然背景上的鼠标开始在屏幕上移动。这是一个严重的警告，因为此时此刻，客户方是不允许用户进行任何合法的连接和系统使用的。

发生了什么事？约翰注意到这个人并不像是管理员或者一般用户，他显然对系统不是很熟悉。约翰怀疑这是个不受欢迎的入侵者。虽不想把入侵者吓跑，但他想确认这个人究竟是管理员还是入侵了同一个系统的另一个黑客。

很快，约翰的目标从渗透测试变成了找出入侵组织内部的恶意黑客。

## 8.6.2 故事

约翰立即决定对该名黑客进行社会工程，并且搜集尽可能多的资料来维护客户的利益。他真的没有时间做十分周密的计划，也没有时间做适当的信息收集。

他冒着很大的风险，打开记事本程序，决定伪装成一名“n00b”黑客，也就是一个新手、技术菜鸟，和对方一样，看到这个口开着就进来了。他截取了一些与黑客对话的屏幕截图。注意看一下图8-1，他是如何对黑客进行社会工程的。约翰先开始对话，次行是黑客说的话。

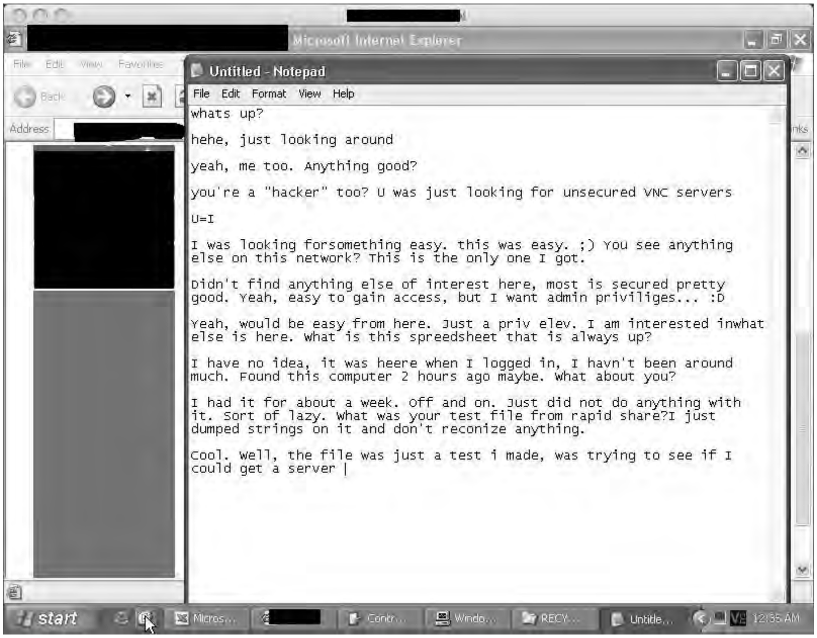



图8-1 事件的屏幕截图

下面是对话的原稿。它很长，其中出现的所有错误和黑话都是未经加工的，但是会揭示出这次攻击的原貌。约翰（宋体）首先开始说话。

– 嗨，什么情况？

– 呵呵，随便看看。

– 呵呵，我也是。有什么好东西吗？

– 你也是“黑客”？你在寻找不安全的VNC服务器。

– 你=我

– 我找的都是简单的系统，这个系统就是。:) 你在这网络中还有什么其他发现吗？我只找到这个。

– 没找到什么有趣的东西，大部分系统都保护得不错。是啊，很容易进来，但是我想要管理员权限…… :D

– 是啊，获取这里的管理员权限再简单不过了，提权就可以了。我感兴趣的是这里还有什么。这个一直打开的电子表单是什么？

– 我也不知道，我进来的时候就是这样了，我还没怎么看呢。大约两小时前刚发现这台电脑。你呢？

– 我发现快一个星期了，时不时进来看看，但还没用它做任何事，有点懒。你在快速共享上的测试文件是什么？我提取了里面的一些字符串，但是看不清。

– 酷。文件是我做的一个测试，我尝试运行一个程序（特洛伊木马），但是被防火墙阻止了。

– 哈哈。我也遇到了相同的问题。我做了个metasploit脚本，但也没有进展，这就是为什么我还在这。你是本地的还是国外的？我知道有些人是丹麦的。

– 我是挪威的，呵呵，我在丹麦有亲戚。

– 你逛什么论坛吗？我以前有几个喜欢的论坛，但后来都消失了。

– 我主要逛编程论坛，其他地方不大去。你做黑客很久了吗？能问一下你的年龄吗？我22岁。

– 我做这个一年左右，主要是为了好玩。我还在上学，16岁，就是找点事做。你去过邪恶地带（evilzone）吗？

– 没有。我做这个也纯粹是为了好玩，只是想看看自己能做什么，测试一下我的技能。顺便说一句，我写了个“VNC探测器”程序，已经找到了很多服务器，但是只有这里还有点意思。

– 哇。你都写了什么代码呀？我能下载吗？你有网名不？

- 我是用PureBasic写的，但发布还为时过早，现在就自己用用，可能以后会共享出来。我可以上传代码，你来编译，但你要先在软件仓库站点下载一些PureBasic编译器程序：P
- 那太酷了。你可以放在irc附带的pastbin站点上，那里可以匿名发帖。我以前没有用过purebasic，只会python和perl。
- 让我想想，我去pastebin站点上传，给我几分钟时间就好。
- 好的，酷！你有网名吗？我的是jack_rooby。
- 网名，有啥用？我不上irc聊天，但你可以通过电子邮件联系我。
- 太酷了。我指的是irc或论坛上用的账号。邮箱也可以。
- 哦，在编程类论坛上我都是用的全名。可能这么做不够聪明。我的邮箱是intruder@hotmail.com。
- 给我发消息，也许我可以加你为MSN好友。
- 会给你发的。认识会编程的人真不错，如果我以后干这种事的时候卡壳了或找到有用的信息，都可以拿来分享。
- 呵呵，是的，现在我们是一伙的了：P
- 酷！pastebin上传好后告诉我。
- http://pastebin.ca/1273205
- 顺便说一声……这还停留在"alpha"阶段，用户界面还没完成，但可以通过一些变量进行配置。
- 酷。我测试下，看看能不能用。谢谢你的共享。如果我做了什么很酷的事情，能发邮件给你吗？
- 好啊，没问题。如果持续运行这个程序几个小时，你会找到很多服务器的。我还编了些代码去检测服务器的安全配置和漏洞，即使有密码保护也能进入系统。这些服务器的检测结果会以“不安全”（insecure）标志显示出来。但有时候也会出错，不安全的其实并非不安全，但这种情况不是很多，你自己测试看看吧。
- 哇。我在这里也看到其他vnc服务器了，但是都要密码。你的工具可以进入吗？
- 只是很少一部分有漏洞的可以进入，但是你必须使用专门的客户端，像这里说的：
- http://intruderurl.co.uk/video/

– 下载zip文件。

– 好的，我会下载看看。太酷了。快速共享中的后门也是你自己写的吗？还是从其他地方得到的？

– 我自己尝试写了大多数的工具，通过这种方式来学习。是的，这是我自己写的，但是还没有完成，我只是想看看能否运行服务器程序，但还不行，呵呵。

– 知道了，我有点想放弃了，但还是觉得应该回来再试试其他方法。我想这里还有些东西吧，但是我没有自己的僵尸网络，有个叫Zoot54的人想卖给我一个，还有人为他担保，但是我根本不信任他。我还不知道怎么写自己的工具，大部分perl和python对于这种windows主机都不起作用，所以我打算用metasploit，但是出现了防火墙错误。你对此有什么想法吗？有什么酷一点的做法吗？还是转向下一台主机？

– Perl和python都是很好的开始，不过我自己没用过。但当你学会一些语言时，学其他的也不难 :P 也许你可以先试试PureBasic，学起来很容易。呵呵，僵尸网络很酷，我想做一个，但是要让它自我传播有点困难，至少在Vista上不容易。可是，我还没打算放弃这台服务器，再尝试一些别的方法，一定能有办法得到更多权限的。:D

– 酷毙了，你就用这台服务器尝试吧，我已经进来好久了，不知道下一步该做什么了。让我看看你会怎么做，我就能学到更多了。这真是太酷了。你有myspace或者facebook之类的账号吗？只用邮箱吗？

– 现在先用邮箱，等我完全信任你以后，也许会在facebook上加你，我没有myspace账号。我会和你保持联系的：)

– 酷，用邮箱也可以。你有命令行通道吗？还是也用这个相同的图形用户界面？这是个多连接的vnc？

– 是的，我只用ThightVNC或者其他工具，确保不会断开其他用户。实际上我不是命令行粉丝，呵呵 :S

– 酷。我用命令行时常常会犯错，导致连接断开。

– 感谢你没把我断开 :D，一开始见你在这乱搞一气的时候，我还想“糟了，撞上管理员了”，呵呵呵……

– 哈，我看过时区设置，这公司在美国中部，所以对他们来说现在是半夜。

– 是的，我也看到了。我还做了网速测试，呵呵。似乎他们的上传速度要大于下载速度，好奇怪啊……但可能会便于DoD攻击。

– 我指的是DoS（拒绝服务攻击）。

– 我还奇怪这个说法是什么呢，还以为是一个很有趣的名称……你进入过这里的其他系统吗？我很早以前看到过一个软件仓库服务器，但是现在已经不在了。

– 我没有发现其他系统。但是我想访问他们所有的网络计算机……可是数量太庞大了，简直像个大学一样。呵呵，我之前输出了“hello world”。

– 哈哈，你发送到打印机还是屏幕啊？这些人要是某天中午看见鼠标在电子表格应用中乱动，一定会吓一大跳的。

– 哈哈，是的。但是VNC服务器不设密码，太白痴了啊？！我向打印机输出了一些东西，希望有人能看到。

– 哈哈，我相信会的……他们不能在没有管理员权限的情况下运行，所以这不是普通用户做的，一定是某个管理员设置的，不然的话我们的后门就能用了，但是它们现在根本不能运行。或者有人更改配置了？

– 嗯，我想你是对的，可能是某个管理员或者怪胎……

– 你靠这个谋生吗？我一直听你说能靠这个赚钱，我想要是我做一段时间，变得更厉害的话，就能靠它吃饭了。你也是这样做的吗？

– 我是靠编程吃饭的，不从事黑客或者安全类的工作。但这是个好主意，人们愿意为测试安全付钱，如果我们做得好的话，或许能靠这个赚一大笔钱。

– 那正是我希望的。我在“有道德的黑客”网站上买了本书，里面有些不错的程序。我不清楚做测试要多大年龄，但是这可能是我从事这些工作的好起点。里面有许多很好的工具，比如metasploit。如果你没看过的话，真应该好好研究下。

– 好的，谢谢，我会去看的：）可是我现在有点累了，呵呵。我不能整天在这简陋的记事本上聊天，呵呵。以后聊，伙计。遇见你真酷，和你聊天很有趣。

– 是啊，在屏幕上看到记事本时还真是吓了一跳。很高兴遇到你，我会发邮件告诉你程序用得怎么样。很想知道究竟会发生什么。祝你顺利，不要被当做坏人抓了哈！

– 呵呵，谢谢，你也是！：）这很有趣，我要把记事本上的聊天内容保存下来，等我一会，哈哈……

– 好的，哈哈，抱歉。

– 再见。

– 再见。

这场闲谈表明约翰能快速地伪装成另一个人。这不是件容易的事，通常需要周密的计划，但是为了维护客户的安全利益、找到入侵者，他不得不将自己伪装成黑客。

最后，约翰取得了黑客的照片、邮箱和联系信息。他将这个恶意黑客报告给了客户，之后系统得到了修正，保证不会再有轻易入侵系统的事情发生。

这个最高机密案例反映了以专业的方式运用社会工程可以很好地保障客户的安全。

### 8.6.3　社会工程框架的运用

这个案例中有趣的是，公司并非黑客的真正目标。他只是在互联网上寻找易攻击的目标，没想到正好碰到了。对外开放访问权限是十分危险的，若不是刚好被渗透测试人员发现，后果该会多么严重啊！

当然，从这个故事中我们也可以学到许多有关社会工程的知识。约翰刚刚进行检测时并没打算使用社会工程技巧，只是想做一个简单的渗透测试。有时候你必须在毫无准备的情况下运用社会工程技能。

约翰为什么能够在没有回家练习的情况下完成这项任务？很可能约翰每天都在使用这些技巧，至少是经常练习，所以才能运用自如。

从这个案例中学到的最主要的一点可能就是熟能生巧。实际上，约翰本可以在遭遇黑客时，告诉对方自己是管理员，他的所作所为已经被记录，其黑客生涯结束了。他可以使用各种威胁方法，可以将恐惧做为主要战术。

但是这样的话，黑客很有可能会逃跑，之后会返回并试图格式化系统，或者造成更大的破坏以掩盖其入侵痕迹。相反，思维敏捷的约翰在目标身上收集了大量有用的信息，随后利用目标的邮箱、姓名以及Maltego软件，掌握了此人的所有活动。

分析这个故事还能学到的一点就是变通，即随着事态的发展随机应变。当约翰开始从这位黑客身上“收集信息”时，他不确定对方是黑客还是管理员。针对他的第一句话——“嗨，什么情况？”，攻击者可以作出多种回答。在不知道对方会作何反应的情况下，约翰没有时间准备，只能用行话，按照黑客的方式作出反应。

约翰考虑得甚至更远。约翰知道顺应别人的效果最好，于是伪装成n00b，一个水平不高的新手，渴望得到一名技艺超群的真正黑客的教导。在满足了黑客的虚荣心之后，约翰诱导他泄露了各种信息，包括他的联系方式和一张照片。

## 8.7 案例学习的重要性

本书仅介绍了几个案例，它们远不是最可怕的。每天，政府、核电站、资产几十亿的大公司、公用电网甚至整个国家都会成为恶意社会工程攻击的受害者，此外，诈骗、身份盗用和抢劫等每时每刻都在发生。

要避免这些悲剧，最好的一个方法就是研究案例，各个领域的专家都使用这个方法。为了研究表现人类情绪的微表情，心理学家和医生会花无数个小时观看录像和采访记录。

说服方面的专家会回顾、分析并研究积极和消极的说服方式。这有助于他们了解哪些微妙之处会影响他人，以及如何运用它们来保护客户。

司法部门将案例学习作为日常工作的一部分，以便了解罪犯犯罪的原因。犯罪调查员会分析和剖析歹徒的每一个方面，包括他们的饮食、社交、思维方式以及行为的原因。所有这些信息都有助于他们理解罪犯的思想。

这也是专业侧写员找到并抓捕“坏人”所使用的方法。同样，专业的社会工程人员不仅通过自己的案例来学习，同时也通过实践中接触到的案例以及新闻报道中的案例来学到很多知识。通过研究案例，社会工程人员能真正看到人们心理上的弱点，明白为什么社会工程框架中的策略会如此容易奏效。这也是我孜孜不倦地更新www.social-engineer.org的原因，这样能够确保框架中包含了最新的故事和案例，大家可以用这些来提高自身的技能。

最后，由于人们天性中的盲目轻信、同情、怜悯以及帮助他人的欲望，这些攻击都成功了。在日常生活和交往中，我们不应该丧失这些品性。但同时，这些特点也常常被恶意社会工程人员所利用。可能听起来我像是在鼓励大家要像机器人一样铁石心肠、冷酷无情。尽管这样能让大部分社会工程人员无从下手，但也会使生活黯然失色。我所宣扬的是，提高警觉、不断学习以及准备充分。

## 8.8 小结

本书宣扬的重点是利用知识来保障安全。只有意识到危险的存在，知道“罪犯”如何思考，同时能够正视并接受“恶人”的存在，你才能真正地保护自己。为此，本书的最后一章将讨论怎样防御和减轻社会工程攻击。

第 9 章

# 预防和补救

前面的章节向大家展示了社会工程人员诱骗目标泄露重要信息的各种方法和途径，同时也描述了社会工程人员用来影响和操纵他人的许多心理原则。

有时在听完我的演讲或是安全培训之后，人们会显得非常恐惧和害怕，他们会这样说："似乎根本没有办法保障安全。我该怎么做呢？"

这是一个很好的问题。我建议制定一个良好的灾难恢复计划和事件响应机制，因为就目前而言，被黑客攻击可能不是"是否"会发生的问题，而是 "何时"会发生的问题。你可以采取一些防御措施，至少在安全战役中给自己一个反击的机会。

减轻社会工程攻击并非只需确保硬件安全那么简单。按照传统的安全防御思路，你会把钱投到入侵检测系统、防火墙、防病毒程序以及其他维护周边安全的解决方案上。可是在社会工程攻击面前，没有任何软件系统可以安装到你的员工和自己身上以保障安全。

本章列出了我为客户提供的预防和减轻社会工程攻击的6大步骤：

- 学会识别社会工程攻击
- 制定提高个人安全意识的计划
- 充分认识社会工程人员意图获取的信息的价值
- 及时更新软件
- 编制参考指南
- 从社会工程审计案例中吸取经验教训

归根结底，这6点旨在创建安全意识文化。安全意识并非是每年花个40分钟、60分钟或90分

钟做一次培训，而是需要创建一种文化或一套标准，让每个人在一生中都坚定不移地运用。它不只关乎工作或“重要的”网站，而是一个人实现整体安全的方式。

本章涵盖了上述的6点，并分析了为什么创建安全意识文化是防御恶意社会工程人员最有效的措施。

## 9.1　学会识别社会工程攻击

防御和减轻社会工程的第一步是了解攻击。你不必深入了解这些攻击，不需要知道如何创建恶意的PDF文件或者如何制造完美的骗局。但是你必须清楚地知道打开一个恶意PDF文件时会发生什么，必须知道通过什么迹象来判断是否有人在骗你，这样才能保护自己。你需要了解威胁以及运用威胁的手段。

举例来说，你十分重视自己的家，尤其是家人。你不会在火灾发生时才开始计划、预防和减轻火灾所带来的危害，而是会提前安装烟雾探测器并设计发生火灾时的逃生路线。此外，你还会对孩子进行火灾逃生口诀训练，“停、放、跑”。你会教他们通过摸门来判断温度以及蹲低身子防止吸入烟雾。所有这些方法都是为了防止一场真正的火灾以及减轻火灾带来的危害所做的准备。

这些原则同样适用于保护你自己和你的公司防御社会工程攻击。不要等到攻击发生后才意识到它们的危害会有多严重。不要认为我在自我推销，我建议定期对员工进行社会工程审计，看看他们是否具备抵御攻击的能力，然后再进行培训。

教导你自己和员工面对此类攻击时，如何像逃生口令那样，做到“停、放、跑”。社会工程人员攻击公司的最新案例是什么？就像知道火灾会对你家造成什么后果一样，了解这些是预防的第一步。要了解现代社会工程人员与身份窃贼所使用的方法有何不同。你可以在社会工程网站www.social-engineer.org/framework/Social_Engineering_In_The_News上查看有关社会工程人员、骗子、身份窃贼等的最新故事和案例。

另一个好方法就是阅读本书。本书包含了社会工程人员所使用的操纵对象的所有方法及原则。书中不仅涵盖了案例及绝妙的黑客攻击事件，还分析了恶意社会工程人员的思维方式和所使用的策略。

你还可以登录社会工程网站（www.social-engineer.org）的资源区观看视频，它们真实地演示了行动的过程。普通用户不需要通过视频了解如何亲自去执行这些攻击，只需了解社会工程人员是怎样进行攻击的就可以了。

一般来说，你越了解攻击的方式，就越容易“随时”识破它们。要了解社会工程人员使用的肢体语言、表情和措辞，这样当听到或看到某人使用这些方法时，你就会马上有所警觉。

你无需耗费大量的时间去学习社会工程方法。然而，时不时花几分钟时间阅读一下社会工程网站或其他网站上的新闻和案例有助于你了解现今社会工程人员攻击公司的方法。

在你对这些知识和审计过程有了基本的了解之后，接下来创建安全意识文化就相对简单些了。

## 9.2 创建具有个人安全意识的文化

2010年7月，我所在的安全专家小组在Defcon第18届安全会议上举办了首次有组织的专业级社会工程竞赛。一群最优秀的、最聪明的人纷纷从世界各地会聚到内华达州的拉斯维加斯，参加每年一次的交流、培训和学习。

我和小组成员都认为，这将是一个举办竞赛的好机会，可以评测美国的公司是否易受此类攻击（对“竞赛”的反应）。于是我们组织了比赛，感兴趣的人都可报名参加，竞赛分成两个阶段：信息收集和主动攻击。

为了保证比赛的合法性和道德性，我们不希望任何人受到伤害，所以规定不准收集任何社保号码、信用卡和个人身份信息。我们的目的不是让任何人遭到解雇，也不是让任何公司陷入窘境，所以我们决定不涉及公司密码或其他与个人安全相关的信息。相反，我们制定了一个有25~30个“旗标”的列表，包括查出公司是否有内部自助餐厅、谁负责处理公司的垃圾、公司使用何种浏览器、用何种软件打开PDF文件等。最后，我们选择的目标公司覆盖了美国的各行各业，如天然气公司、科技类公司、制造商及零售商等。

每位参赛选手都会被秘密地指派一个目标公司，他有两周的时间去做被动的信息收集工作。这就意味着选手不能联系公司、给他们发邮件，也不能尝试用其他社会工程方法收集信息。相反，他们必须使用网络、Maltego和其他工具收集尽可能多的信息，最终完成一份专业的报告。

通过收集到的信息，我们希望选手能找出一些能够在现实世界中合理运行的攻击方法。然后选手必须来到拉斯维加斯的Defcon大会，坐在一个隔音的电话亭里，打25分钟的电话给他们的目标，实施攻击，看看可以得到什么信息。

我原本可以在接下来的20~30页中告诉你竞赛中发生了什么、结果是什么，但我只想说一件事，那就是每个选手都从目标那里获得了足够的信息，这些公司都未通过安全审计。不管选手的经验和伪装处于什么水平，他们都成功完成了预设的目标。关于这次竞赛的详细报告，请浏览www.social-engineer.org/resources/sectf/SocialEngineer_CTF_Report.pdf上的有关文档 。

这里要提到的就是安全意识。关注安全问题的公司有员工培训项目，以培养他们提防来自电话、互联网或者个人的潜在安全风险的意识。但我们发现这些公司的安全意识还是很薄弱。为什么？世界500强企业在安全、培训、教育、服务上花费了数百万美元，可为什么雇员的安全意识还是不够强呢？

这就是本节标题所提到的，安全意识不是员工的个人意识。在安全实践中，我经常和雇员聊起他们对攻击事件的看法，他们的反馈常常是：“这些又不是我的数据，我担心什么？”这种态度表明了公司想要灌输安全意识却没能切中要害，没有引起重视，没起到效果，最重要的是，没有与个人挂钩。

回顾能找到的许多所谓的安全意识培训材料和方法，我的感觉就是无聊、愚蠢，无法引起参与者的互动或思考。短暂的DVD演示涵盖了太多内容，试图在短时间内给观众灌输过多的细节，却很难深入讲解。

不管你是企业还是个人，我要给你一个挑战，那就是设计一个培训计划，通过互动模式让人们融入其中，并引发人们对安全意识的深思。不要只是告诉员工为什么要设定一个又长又复杂的密码，要让他们见识一下破解一个简单的密码是多么地容易。协助客户进行安全意识培训时，有时我会让一名员工上来，在电脑里输入一个他觉得安全的密码。我会在讲密码安全之前这样做，然后在讲的过程中破解这个密码。通常来说，1~2分钟内密码就会被破解，然后我会向大家公开这个被秘密输入的密码。迅速破解密码会给每个人带来巨大的震撼。做几次类似这样的演示之后，员工就会表示现在他们知道密码安全是多么重要了。

当讨论电子邮件中的恶意附件攻击时，我不会向员工展示如何构造一个恶意PDF文件，而是会向他们展示当恶意PDF文件被打开时，受害者和攻击者的电脑中会出现什么。这可以帮助他们理解一个简单的崩溃如何导致一场灾难。

当然，这种教学方式会引起极大的恐慌情绪。尽管这不是我的目的，但也并不是一个可怕的结果，员工会因此记忆深刻。培训的目的是让他们理解不仅要在使用办公室电脑时这样做，也要在应用个人银行账户、家用电脑时这样做，树立起自我安全意识。

希望每个听过我安全演讲或者读过本书的人都审视一下自己是如何使用互联网的，反复使用的密码是否修改过，密码和个人信息是否存储在了不安全的位置，以及用互联网连接了哪些地方。我曾无数次看到有人坐在星巴克咖啡馆里，使用免费的Wi-Fi连接登录银行账户，或进行网络交易。我很想起身朝那个人大叫，告诉他如果有个坏人进入了同样的网络，他的整个生活就会天翻地覆，但是我没有这么做。

我希望读到这里的人也可以想想自己是如何通过电话泄露信息的。骗子和诈骗专家用许多方法窃取老年人、经济困难的人和其他人的信息。打电话仍旧是一个强有效的方式。充分认识厂商、供应商和银行的政策，了解他们会不会通过电话询问信息，可以帮你避免掉入许多陷阱。例如，许多银行在政策中申明他们永远不会通过电话询问社保号码或银行账号。知道这些有助于你保护自己，以免被骗而变得一贫如洗。

培养安全意识是一个持续不断的过程，需要你安排时间去不断地学习。在了解所有这些有用的信息后，你可以用它们来制定一个计划，以保护你的安全。

## 9.3　充分认识信息的价值

再次回顾一下Defcon第18届安全会议上的社会工程竞赛，我们还可以学到一条宝贵的经验教训，即当认为信息无用或价值很小的时候，人们就不会付出精力对其进行保护。

这一点虽已反复强调，却被无数次证明是正确的，因为很多目标会心甘情愿地泄露有关餐厅、垃圾处理等的信息。你必须意识到自己手中数据的价值，以及社会工程人员所使用的有意贬低数据价值的战术。

在向某人提供信息前，要判断与你通话或者交涉的这个人是否有得到信息的必要。人类天生乐于帮助那些我们认为需要帮助的人。这是社会工程人员操控目标获取有价值信息的主要手段。分析与你进行沟通的人，判断他是否有权获得他想要的信息，可以免去因上当受骗而带来的尴尬和伤害。

举例来说，在Defcon社会工程竞赛中，一位参赛者伪装成一家经营杀毒产品的大公司的顾客，声称遇到了一个严重的问题——电脑不能上网了，他认为这是由于杀毒软件引起的，希望技术支持代表能做一件简单的事帮他解决这个问题——浏览一个网站。

恶意的社会工程人员经常使用这种攻击方式。通过驱使目标访问一个嵌入恶意代码或恶意文件的网站，他能够入侵目标的计算机和网络。在竞赛的案例中，网站本身并未嵌入恶意代码或文件，但需要强调的是，如果这是场真的恶意攻击的话，那就成功了。

参赛者所做的第一次尝试如下："我无法浏览网站了，我想是你们的产品造成的。你能访问一下这个网站吗？看看到底是否是由你们的软件引起的。"

技术支持代表彬彬有礼地回答："先生，我们的产品不会阻止你访问站点，我是否能访问都不能说明问题。"他拒绝了要求。

参赛者没有放弃，几番交谈之后他再次尝试："你说你们的产品不会阻止我访问站点，但是我是安装了你们的软件之后才不能访问的，所以能请你帮我检查一下吗？"

对方再次拒绝了他的要求："先生，对于你的不便我很抱歉，但是我们的产品绝对不会阻止你访问站点，即使我能访问，也不能帮你解决问题。"

似乎请求会以被拒绝而告终，但参赛者打算再做最后一次尝试："先生，如果你能帮我看看网站我会感觉好过些的。请你帮我看看吧，可以吗？"

这个简单的请求让技术支持代表失控了，最后他打开浏览器，访问了那个网站。一开始，他有准确的判断，甚至有一定的安全意识并作出了正确的回答，但是最终还是因为想让"顾客感觉好过些"而接受了他的要求。如果这是一次恶意攻击的话，这将导致公司遭受巨大的损失。

技术支持代表知道对方的要求与对方电话中所说的问题关系并不大。与他一样，你必须判断并分析对方要求的信息是否是他应该得到的，是否与他息息相关。换一个角度看的话，如果参赛者是一名合法的顾客，技术支持代表拒绝了他的要求，最坏的结果是什么？

顾客在被拒绝后一定会表现出不悦，但这并不会改变结果，他所用的产品并非他痛苦的根源。

社会工程人员经常用天气、工作及产品等话题套近乎，然后挖掘想要的信息。这就需要用安全意识策略来应对——针对骗子可能运用的伎俩对员工进行培训，使他们消除因拒绝客户而造成的顾虑。

在一次审计中，我伪装成CFO的助理。呼叫中心的员工通常会担心因拒绝高层的要求而丢掉工作。为什么？因为他们没有接受过适当的培训，不知道拒绝并不会影响他们的工作。同样，应该为员工提供一份方案，告诉他们什么样的信息要求才是合理的。

受过培训并且具有安全意识的人知道，即使是不起眼的信息也可能造成巨大的损失，因而会对信息价值作出准确的判断。如果知道电话那头的人其实并不需要知道自助餐厅的食物供应商是谁，员工就可以作出恰当的回答。如果你是雇主，就应该帮助员工制定应对这些要求的合理回答。大多数情况下，简单的一句回答就能粉碎社会工程人员很多的阴谋，比如回答说："对不起，我没有此项信息。如果你想知道，请联系采购部。"或者"对不起，我没有提供该信息的权利，你可以发送邮件至info@company.com询问。"

之前提到社会工程人员会营造一种氛围，使目标觉得信息并非具有很大的价值，从而吐露这些"不重要的"信息。

再举一个竞赛中的例子，一位参赛者被要求提供身份信息。他伪装成受雇为对方公司做内部审计的人员，当目标想要核实其身份时，他将话题转到了申请表上。参赛者假装对他的一个同事说："简，XX公司的一位先生想知道申请书上的ID号，你能帮忙从比尔桌上拿一下吗？"

当"简"去取参赛者要求的表格时，参赛者开始与目标闲聊。开始时聊的是"得克萨斯州的天气怎么样啊？"、"你去过查理酒吧吗？"诸如此类的话题，可慢慢聊到了"自助餐厅的食物谁管啊？"及"想看看我们做的超酷网站吗？"。

这一切的闲聊都是为了"等待"ID号。社会工程人员每天都会用这种方法。转移注意力与施展魅力是伪装的关键手法。在"闲谈"中透露的信息通常被认为是没有太多价值的，因为人们的注意力根本没有放在那里。如果社会工程人员是在"核实审计信息"时问同样的问题，则对方的态度可能大不相同。但正因为谈话的氛围很友好，信息才能在无意中被泄露。

对抗这种社会工程策略的正确方式就是不管对话的哪个阶段，都要思量你打算透露的信息的价值。在之前的例子中，目标在得到ID之前应该避免闲谈，这样的态度才是恰当的，才可以防止受骗。

要做到这点并不容易，因为工作中的员工，特别是那些面向客户的员工，不可能因为害怕攻击而不透露任何信息，所以仅仅意识到信息的价值并不能阻止攻击的发生。

## 9.4 及时更新软件

大多数企业都必须向公众和客户发布一些信息。即便就我的业务而言，我也必须公开电话号码、电子邮箱和网站地址，必须收发PDF文件，必须能够与客户、供货商以及厂商在电话中沟通自如。

然而，前面提到的观点表明向公众公开此类信息就意味着公司与隐私的终结。要想公布某些信息，同时又不会造成信息泄露，应该怎么办呢？

不断更新软件。在竞赛中，60%以上的公司还在使用IE6和Adobe Acrobat 8。这一数据真是令人震惊啊。

这两款应用软件中存在大量公开的漏洞。如果知道目标使用这两款软件，就可以对其发起大规模恶意攻击，连入侵检测系统、防火墙以及杀毒软件都无法阻挡。但是你知道有效的防御措施是什么吗？

答案就是更新升级。软件的最新版本通常修补了其安全漏洞，至少是其中的大部分。如果某款软件的安全记录很糟糕，尽量不要使用它，请选择一些漏洞较少的软件。

问题在于公司怠于进行软件更新。IE6是一款相当古老的软件，微软差不多已经停止对它的安全更新支持了。[①]Adobe 8有几十个已经公开的漏洞。这只是我们在比赛中发现的众多软件中的两个。然而，现实是你不得不发布信息，你必须能够自由地告诉别人你的近况。为了减少担忧，你必须确保你和员工都及时更新软件。

在竞赛中的打电话环节，如果某个员工透露了公司使用的是Firefox、Chrome或其他安全浏览器，又或者是FoxIt或最新的Adobe软件，参赛者就将无从下手了。我并不是说那些软件本身不存在任何问题，某些版本的漏洞肯定仍然存在，但是这些软件明显要更安全。获得这部分信息还是有价值的，只是如果没有漏洞可以利用的话，就无法启动下一步的攻击了。

及时更新软件这一提醒可能会遭受巨大的抨击，因为它的工作量很大且耗资巨大。在旧版本软件依然在运行的情况下更改内部规则和方法是十分困难的，这可能会引起内部系统的整体转换。

然而，如果公司在安全方面不遗余力，并且要树立员工的个人安全意识，那么渐渐地这些变化就将成为企业文化的一部分。

① 由于IE6的安全问题，微软在2011年初发布了一个有关停止使用IE6的倒计时站点（http://www.ie6countdown.com/），建议用户尽快停止使用IE6。——译者注

## 9.5 编制参考指南

另一个值得一提的做法是编制参考指南。不要畏缩，我并不是指在A和B同时出现的情形下，员工必须回答X。我的意思是给出指导大纲，帮助员工进行批判性的思考。考虑如下情景。

如果某人声称自己是CEO的手下，要求你提供密码，该如何应对？如果某人没有预约，但外表和行为上看上去像供应商，他要求进入大楼或其他地方，该怎么处理？

在遇到这些情况时，参考指南能帮助员工作出恰当的反应，并且让他们应对自如。举个例子，有一本参考指南如下。

如果某人打来电话声称自己来自管理层办公室，要求你提供一些信息或内部数据，可以按下列步骤操作。

(1) 询问来电者的员工号和姓名。在得到反馈前不要回答任何问题。

(2) 获取身份信息后，询问他需要这些信息的项目号。

(3) 如果(1)和(2)都对答如流，就可以为他提供信息。如果答不上来，要求他的经理发一份邮件给你的经理申请授权，然后终止通话。

类似这样的简单参考指南可以帮助员工明白在考验其安全意识的情况下该说什么以及该做什么。

## 9.6 学习社会工程审计案例

如果你有过骨折的经历，就知道在恢复时医生会为你安排一些康复理疗。在康复师进行恢复性理疗时，你会进行一些压力测试。这种类型的测试会帮助医生发现你还有哪些薄弱之处需要加强。同样的方法也适用于公司，只不过社会工程审计不是在“损坏”发生后再进行“测试”，而是在入侵破坏发生前所做的测试。

以下小节回答了一些有关社会工程审计的重要问题，并且阐释了如何选择最优秀的审计人员。在深入学习社会工程审计之前，你需要知道审计的真正含义是什么。

### 9.6.1 理解什么是社会安全审计

社会工程审计的基本定义为，雇用专业安全人员模仿恶意社会工程人员所使用的攻击方式对企业中的人、规章以及物理环境所进行的安全测试。恶意社会工程人员与专业安全审计人员主要有三点不同：

- 通常，专业的安全审计人员会遵循道德与法律上的约束。
- 专业安全审计人员的目的是帮助客户，而不是窃取客户资料、使客户陷入窘境或者伤害客户。
- 专业的安全审计有一定的范围限制，而真正的攻击者则不受这些限制。

专业的安全审计人员会花费大量的时间去分析和收集“目标”或客户的信息，然后使用这些信息展开真实的攻击。在此过程中，专业的安全审计人员会牢记审计的目标。这是很重要的一点，因为他们可能会偏离路线，从而给社会工程人员和目标都带来可怕的后果。明确定义的目标可以避免社会工程审计人员犯这种错。

### 9.6.2　设立审计目标

专业社会工程人员的行为必须符合道德和伦理，同时又要跨越界线，戴上真正的“黑帽”，暂时担任恶意社会工程人员的角色。这就意味着需要注意他能利用什么手段入侵公司并暴露公司防御的漏洞或弱点，不管手段有多么低下。

在寻找安全漏洞的同时也要考虑员工。在社会工程安全审计中被入侵的公司通常认为解雇那个在攻击中上当的员工就能修正问题，堵住漏洞。客户没有意识到的是，审计过后，在审计中犯过错的员工很可能成为大楼中安全意识最高的人。

专业社会工程人员必须采取额外的防范措施，确保员工不至于被开除。我个人的做法是尽量不透露责任员工的姓名，并且告诉客户审计的关键点不是员工。如果我无能为力，必须透露员工的姓名，那么在报告中我会重点强调，是公司的培训、规章和防御不完善才导致员工“犯错”。

一般的社会工程审计绝不会对员工落井下石，摧毁他的名誉和生活。和审计人员制定审计目标时，我会针对关键方面列出从0到10不等的强度等级：

- 判断员工是否会点击或打开来自陌生人邮件中的链接或文件
- 判断员工是否会登录某个网站，输入个人或业务相关的信息
- 判断通过电话、在工作场所、个人场所（即酒吧、体育馆、托儿所）或面对面的交流可以从员工口中获取多少信息
- 判断办公环境中的锁、摄像头、传感器和门卫的安全等级
- 确定社会工程人员是否有能力构建一个恶意U盘或DVD，并诱导员工把它用在他的工作电脑上

当然，可以审计和测试的领域很多，但是我只能尽可能列出企业所要求审计的目标。我发现，企业通常不知道他们需要什么。审计人员的职责就是为公司介绍多种入侵公司的方法，然后确定他们到底需要测试哪些方面。

明确目标后，还要列出一张表单，注明审计中不应该包含的事项。

## 9.6.3 审计中的可为与不可为

检测企业是否存在安全漏洞可以采用多种不同的测试方法。运用本书中所有的原则，可以帮助你编制出一个不错的攻击计划。但是在策划攻击时，需要避免以下几点：

- 攻击目标的家人和朋友
- 伪造犯罪或不忠的证据，让目标名誉扫地
- 根据当地的法律，冒充执法人员可能是违法的
- 闯入目标的家或公寓
- 利用目标的风流韵事或窘迫状况进行敲诈

这样的事要应该不惜一切代价来避免，因为它们与审计目标不符，而且让被审计方有种被侵犯的感觉。然而问题来了，如果在审计过程中出现了诸如此类的证据该如何处理。每个审计人员必须自己决定该如何处理，但也不妨参照一些例子。

在一次审计中，审计人员发现一名员工利用公司的高速网络下载色情影片到外部硬盘中。该员工可能因此被解雇，但审计人员并不想这种结果出现，所以只是过去警告他停止该行为。该员工显得很尴尬、沮丧，并且认为审计人员还是会揭发他，于是决定先发制人、倒打一耙，他跑去和老板说审计人员故意在他的电脑中植入了这些让人反感的证据。

当然，在纠纷发生时，审计人员有日志和屏幕截图为证，最后那名员工还是被解雇了。同时，审计人员也受到了批评，因为公司严令禁止该员工的行为，而审计人员在发现证据时没有第一时间报告。

在另一个案例中，审计人员发现有人下载儿童淫秽视频并在互联网上传播，而且在该人的电脑上同时发现了他妻子和孩子的照片。他知道如果揭露此事，可能导致他妻离子散，身陷囹圄，家庭和事业就此毁于一旦。

当地的法律规定，传播儿童淫秽视频是违法的，而且在道德上也属于恶劣行径。审计人员将此事告知公司和权威部门，该男子因此失去了事业、家庭以及自由。

明确列出“不可为”的事项来强化审计活动，能使你在法律与道德的边缘把握住正确的方向。在与身体语言大师乔·纳瓦罗（Joe Navarro）的一次会面中，他就此发表了自己的观点。他指出，除非你是执法者，否则在介入某事件前，必须决定什么可为以及什么不可为。那么审计人员应该在审计中做些什么呢？

- **网络钓鱼攻击** 有针对性的邮件攻击，查看员工是否容易受到恶意邮件攻击。
- **现场伪装攻击** 选择精确且可控的伪装，然后进行电话或面对面攻击，测试员工是否容易上当受骗。
- **引诱** 一种在设法进入目标建筑物或其他设施后的现场攻击，将包含恶意代码和文件的U

盘或DVD光盘放在现场，测试有没有人上钩。

- **尾随**　一种现场攻击，审计人员试图尾随一群公司员工混入大楼。
- **物理安全（红队）**　试图通过物理方式进入办公室，获取公司有价值的资产或信息。

这个清单可以帮助专业审计人员确立指南，列出在审计中什么可为、什么不可为。此外，许多公司还面临的一个最大的问题是，如何挑选优秀的审计人员来完成这些任务。

### 9.6.4　挑选最好的审计人员

如果你摔断了骨头，病情十分严重，医生告诉你痊愈的机会只有50%，但是如果是非常出色的医生来医治的话，痊愈的几率会增加，你会尽力寻找这样一位医生来医治你吗？当找到他的时候，你会问什么问题？你不想看看他过去的工作成就吗？你会想要一些证据，证明他具有理论和实践能力，能提高你康复的机率。

你可以依照类似的方式，找寻合适的审计人员。在与审计人员交流时，以下问题可供参考。

- **知识**　这个团队是否发表过研究报告、论文、演讲或者其他显示其社会工程知识的材料？他们是否是这个领域的领先者？你不应该安全审计工作交给那些使用过时方法、不能与时俱进的团队。

  不经过一番调查，很难判断一名审计人员和一个审计团队的知识水平。询问他们是否发表过有关安全审计的论文、文章等是一个不错的主意。确保你雇用的团队是这个领域的佼佼者。
- **经验**　客户通常不愿意被指名道姓、大肆宣扬。以我的经验来看，许多客户不愿被放上网站或市场宣传材料中，因为他们会感到尴尬，也怕导致入侵事件的发生。但你可以通过其他方式判断审计人员的经验。不妨询问他曾使用过的方法以及解决方案。

  审计人员在初次会面时通常不会将所有的秘密全盘托出，但是多问一些他进行过的攻击，能帮助你判定他的技能水平。
- **合同**　为审计活动列出框架、形成文件并设定相应的限制，是审计成功的前奏。个人而言，我不喜欢大量的限制，因为大部分恶意社会工程人员根本不讲什么限制。但至少应该就一些规则和不允许的条目达成一致。

  社会工程人员希望对方准许其进行电话录音，在巡查建筑物或交互的过程中进行录像，尤其是在进行物理安全审计时，可以获得从办公场所拿走一些东西的书面许可。审计人员可不想在完成审计任务后得到一张逮捕令或一份起诉书。

  同时要指派紧急联系人，他知道审计一事并且能为审计人员和他的团队担保。如果审计人员陷入法律纠纷，他可以打电话给紧急联系人。没人想在半夜翻垃圾的时候被警察抓去蹲拘留所。有了紧急联系人，就等于有了“免于司法纠纷”的通行证，长久来看这能省去许多麻烦。
- **共识**　运用本书中的原则去寻找优秀的审计人员。与他通电话或见面时，他给你什么感觉？你看到了什么？你有没有感觉他非常专业，他的目的就是要帮助你？

审计团队对自己的描述和业务方式与你的要求一致吗？如果你是雇用审计人员的项目经理，责任都需要你来承担。审计人员也许不想和整个项目组的人见面，因为越少人知道社会工程团队的外貌，对物理安全审计就越有利。所以他们可能只想见项目组中的一到两个人。这就意味着你必须确保审计人员的素质很高，有足够的能力完成任务。

- **时间** 公司在寻找审计人员时经常会犯一大错误，即不给审计人员足够的时间去完成工作。他们认为打几通电话、上一下网站完全可以在一天内完成。尽管这可能是真的，但是如何进行信息收集、计划和目标研究呢？这些都需要花时间的。时间非常重要，但也是把双刃剑——足够的时间有利于审计工作更好地完成，但时间太长会增加成本。管理，但是不要微管理。

这些只是在为公司挑选合适审计队伍时所要考虑的一部分问题。最后，社会工程团队必须让你感到舒服和满意，让你相信他们是真心想帮助你，他们将尽全力保持专业并遵守规则。

## 9.7 总结

如果不将知识用于实践，它就没有任何价值。

——安东·契诃夫

本书中提供的知识并不是轻轻松松就能掌握的。许多知识揭示了人们的思考和行为方式存在严重的漏洞。当我和我的导师马蒂共同教授安全课程时，他介绍了一种日语名为“shikata ga nai”的负载编码器，意思是“没办法了”，或者粗略翻译为“没希望了”。

我曾想过将这个短语作为本节的引语，但我认为“没希望了”带有强烈的宿命论色彩，也和我通常的价值观相违背。相反，我觉得契诃夫的这句话更符合本书的主题。我曾反复声明，完善技能并在实践中检测这些技能远非掌握知识这么简单。如果你过于害怕本书中提到的内容，就会对人们被攻击的方法感到愤怒，而这只会使你固步自封。我建议你撇下恐惧，从另一个角度认识本书中的内容：换一个心态，鼓励自己学习、思考并理解“坏人”所使用的方法，从而保护自己不受他们的侵害。

我并不是说已经没有任何可怕的了，适度的恐惧还是必要的。保护你的资料、个人信息和身份信息，同时理解“黑客”的思维方式以及本书中提供的信息，可能会对你更为有利。

我希望你能够在生活和工作中运用以下几个小节的内容，如果你负责公司和客户的安全，更应这样做。此外，阅读这部分内容也有助于你保护自身的安全。

### 9.7.1 社会工程并非总是消极的

我希望读完本书之后，社会工程留给你的印象不是消极的。不仅是黑客、骗子在使用社会工

程策略，医生、心理医师、社会工作者、父母、孩子、老板、员工……每个人都会或多或少地运用社会工程策略。说服就是日常社交生活中经常使用的策略。

要知道社会工程并不总是可怕、黑暗和邪恶的，这对了解社会工程技能的使用方式大有帮助。了解、实践并精通这些技能后，你就能轻松辨别它们是如何被用来攻击他人的了。

你可以在黑暗角落以外的地方分析这些技能。你可以阅读心理学、说服和销售方面的书籍，了解这些技能在该领域是如何被运用的。

### 9.7.2　收集与组织信息的重要性

我觉得信息收集的重要性再怎么反复强调也不为过。每一个社会工程项目的质量、专业性以及成功正是取决于信息收集的水平。网络是浩瀚无边的信息源。公司会将财务记录、员工的姓名和职位、联系信息、公司的照片、安全规章、合同、厂商和供应商的名字、人们的个人资料等都发布到网上。员工和普通人也会将私人的照片、地址、购买的东西、租约、合同以及喜欢的食物、团队和音乐等信息放到网上。

掌握了大量的信息之后，社会工程人员可以从中挑选出想要使用的那些，并决定使用什么攻击方式去对付目标。接下来，根据收集到的信息，社会工程人员能设计出针对目标最有效的故事情节和伪装。没有本书反复强调的信息收集工作，社会工程活动很可能以失败告终。

举例来说，如果一个专业的审计人员有一项期限为3周的工作，他应该在信息收集上花去一半的时间。不过，专业的审计人员经常采用使用过的伪装去吸引和接近目标。不要养成这个习惯，在信息收集上多花些时间吧。

与信息收集同样重要的是信息的存储与分类，也许可以使用第2章中提到的方法。不但要学会高效地收集信息，还要知道如何存储信息，这对在实战中高效使用信息大有裨益。不能只是简单地把信息存储在一个文档中，要将它们归类并做上标记，这样信息使用起来会更加方便，特别是在电话攻击的时候。

请牢记，社会工程人员表现的好坏取决于他所获得的信息。我曾见过许多社会工程活动最后都功亏一篑，就是因为信息收集得不当或不全。我也见过许多并不是很出色的说服者或不够有魅力的人，最终因为收集了确切的信息而力挽狂澜。

信息是社会工程的关键，如果你只从本书中学到一点，那么一定要是这一点。

### 9.7.3　谨慎用词

就像9.7节开篇所描述的，没能投入使用的信息毫无价值。你可以收集所有的信息，然后进行组织和分类，但是你也需要高效地利用它们，为此第一步就是组织你将使用的语句。

之前讨论过诱导和铺垫。这是两种非常重要的技巧，我希望你们多练习使用。使用心锚、关键词和话语为目标灌输感情和想法，使他听你的话。铺垫是一种威力强大的技巧，短时间内并不容易掌握，但是熟能生巧。铺垫的好处是你可以随时随地练习，比如在家、在工作中针对孩子、父母和客户进行练习。

不要认为练习就是要求别人做其不愿意做的事情。要用铺垫来激发别人对某个建议或想法抱有更加开放的态度，而不要恶意地使用它。孩子总是这么做，例如你的女儿说："爸爸，我爱你……"过了几秒又说道："我能要那个新玩具吗？"这就是个铺垫的例子，将"目标"置于一种乐意接受的情感状态下。

一旦掌握了铺垫技巧，或者精于使用铺垫，就可以在你的诱导中加以使用。记住，没有人喜欢被审问的感觉。诱导不是模仿警察审问，它应该是流畅地交流，在不知不觉中完成对目标和主题的信息收集。

学习日常交谈中提问的方法和步骤，不仅能增强社会工程技能，也能提高交流水平。人们喜欢他人关注其生活和工作。将这一技能用于好的方面，可以强化你的社会工程能力。

我有一个好朋友，她能让人们告诉她任何事，这是非常不寻常的。完全陌生的人也会这样，在谈话的最后他们还会奇怪："我真不知道为什么会和你说这些事……"她并不是一个社会工程人员，也不做安全方面的工作，但她是个优秀的诱导者。

掌握铺垫和诱导技能也能提高斟酌言语的能力。这些技能能让你以更加智慧、不那么冒昧的方式寻找和收集信息。

### 9.7.4 巧妙伪装

记住，好的伪装并不是纯粹的说谎和编故事，而是在短时间内变身成为所伪装的角色。你的一切，包括想法、动作、说话方式和动机，都应该体现所伪装角色的特征。如果你做得足够好，就会取得目标的信任。

另一点要牢记的是，伪装并不只是运用在社会工程中，在生活中也会用到。想象一下这个场景：你刚刚和配偶发生了一番争吵，上班时你不想让任何人知道家里发生了不愉快，所以当同事跟你打招呼说"嘿，吉姆，今天好吗？"时，你的回答会是"很好"。

这与事实正好相反，但你怎样做才能使之变得可信呢？对人微笑，通过手势和肢体语言传达出自信。如果你非常紧张自己的隐私，不想与同事分享太多，你甚至会编造出一个"欢乐的故事"，证明你的生活有多么美好。

这只是一种情况，可以说人们一直在运用伪装。任何时候，只要你试图向人们展示与事实不符的表象，你"编造的故事"就是一种伪装。当然，大多数人不善于此，常常露出破绽，但是在

生活和工作中注意这些情况，能为分析伪装打下基础。

分析这些情景能帮助你找出伪装中需要提高的地方，有助于你掌握这项非常有用的技能。

### 9.7.5　练习解读表情

我想我可以用几周的时间来谈论微表情。这个话题让我着迷，让我觉得人类有一种内置的机制，可以暴露内心最深处、最黑暗的感觉，而且大部分人都控制不了它。我们的情绪会引起某些肌肉的收缩，从而呈现持续时间为几毫秒的表情，这只是造物主惊人的创造。但是学习注意、读懂并利用这些表情来操纵他人才真正是一门惊人的学问。

练习第5章中讨论的再现微表情的方法。练习的过程中，要注意微表情让你产生的情绪。练习这些表情能帮你读懂其他人的表情。

在练习的过程中，不仅要重视解读他人的微表情，也要注意控制自己的微表情，防止他人读懂你内心的想法。请牢记，解读他人的表情是一种不错的技能，但是掌握自己的微表情、肢体语言和语调是一种更厉害的技能，此技能可以提高你在安全实践和个人社交方面的水平。掌握这些技能后，你就能渐渐体会如何运用第5章中的主要概念之一——人类思维缓冲区溢出。从一个更高的层面来看，人类思维的工作方式很像软件，它也像软件那样可以被模糊测试、检测和颠覆。请重读5.6节，确保你已充分理解该节中提出的原则。

### 9.7.6　操纵与影响

操纵和影响是社会交往的两个重要方面，会对你接触的人产生巨大的影响。出于这个原因，在使用第6章中的信息时需要特别注意。学会怎样说服和操纵他人对社会工程活动的成败至关重要。每天，人们都在尝试操纵和说服他人去采取某些行动，其中某些不好的行为会给他人造成金钱损失，甚至是个人自由和身份信息的丧失。

将那些场景作为教学工具。分析营销人员、心理学家、律师、教师甚至是同事操纵你的方法。从中挑出你能学习的几点，为你所用。

记住，说服并不总是消极的，它不一定意味着让人们去做他们不愿意做的事情。说服也有积极的影响，很多时候积极的说服更难办到。如果你掌握了这些技巧，并用之来帮助人们维护安全，那当遇到其他人使用消极说服策略时，你可能一眼就会识别出来。

### 9.7.7　警惕恶意策略

充分了解攻击者会使用什么样的策略可以让你免于入侵之害。专业的审计人员可以使用这些策略培训客户如何发现可能的攻击迹象。请保持警惕，谨慎找出这些策略的应用实例。

例如，“坏人”使用的一种策略就是乱中取胜、浑水摸鱼。当飞机撞上世贸大厦时、当海地遭遇地震袭击时、当亚洲碰上海啸灾难时，很多人因此而丧生，其他人的生活、心灵和感情则遭到了沉重的打击。在这些人们脆弱无助的时候，坏家伙们就会出现并发起攻击。

举个例子，我读过一篇有关狮子在野外捕猎的文章。文章中说，狮子会在一群猎物中制造混乱，然后选择一个受害者。它会朝地面咆哮，而不是向着猎物或者天空，为什么呢？这是因为巨大而令人恐惧的咆哮声会在地面产生混响，猎物们会很迷茫，不知道狮子究竟是从哪个方向来的。结果有些猎物会向左逃窜，有些则会向右，惊慌之中丢下那些年幼、年迈、体弱和未发育成熟的群成员。

这与恶意社会工程人员的手法大同小异。他们以“咆哮”的方式引起或增加混乱。他们利用那些帮助寻找在灾难中逝去亲人的网站，或者声称自己在灾难中失去了家人和朋友。当情感被迷惑时，“目标”就不能识破攻击了。

毫无经验和技术不成熟的受害者首先会给出少量信息，攻击者会据此找到攻击入口。接下来攻击者会发动进一步的攻击，而这些攻击会更加邪恶和残酷。

请留意这些情况，保护你的客户和自己不成为他们的受害者。同样，将这些情况作为课程来学习，分析其中所使用的方法，观察它们是否奏效。如此一来可锻炼你的能力，提高对潜在威胁的警惕性。

不幸的是，狮子与社会工程人员的差异（除了明显的差异外）是社会工程人员从来不会大声嘶吼，他不会在那里大喊：“我要捕猎，你们快跑！”恶意的社会工程人员总是悄无声息地，每年将成千上万的人引入他们部署的精妙的攻击圈套中。

### 9.7.8 利用你的恐惧

如果本章内容或多或少给你带来了一些恐惧感，我会说“很好”。你需要恐惧，因为适当的恐惧能拯救你的生命，至少可以保护你的身份信息和公司。

积极地利用恐惧，切忌生气和消沉。制定一个改变自我的计划，然后培训自己、家人和员工，学会观察、提防和防御这些攻击。下决心一定不能让自己或公司受到攻击，然后尽量做到这一点。

本书的宗旨可以归结为“安全之本在于教育”。人性攻击是一门艺术，而社会工程是科学、艺术和技能的综合体。如果各种因素搭配得当，结果就是“shikata ga nai”（没办法）。

每年入侵事件给企业造成数百万美元的损失，其中绝大多数的入侵事件都来自社会工程攻击。然而，一种普遍的现象是，当我们希望在渗透测试服务中加入社会工程审计时，他们却拒绝了。

为什么？

企业通常害怕改变。在专业实践中，我无数次地听到聪明且成功的老板这样说道：“我们不需要

社会工程审计，我们的员工不会落入那些圈套的。”然后，在渗透测试中我们会通过打电话（已被准许）套取信息，之后当我们在报告中披露这些信息时，他们会对套取信息竟然如此简单惊叹不已。

在各种企业中，各级员工的安全意识并没有太大的不同。当渗透测试之后，我们和公司说起我们组织的一个安全意识培训项目时，许多人告诉我们，公司从未对呼叫中心和技术支持部门的员工做过正式、认真的培训。而这些部门常常是社会工程攻击的首选目标。

这正是我所说的问题的关键所在。通过培训建立安全意识并非是一句口号，它必须成为一项使命。只有公司以及公司的员工将安全当做自己的事情来认真对待，这个问题才能真正得到解决。与此同时，那些带着严肃态度阅读本书、渴望窥探社会黑暗角落的人，一定能够提高技能，从而使其家庭、自身和公司更加安全。

当“狮子咆哮”时，请成为那个带领大家逃亡的人吧。做一个知道如何应对和防御攻击的榜样。

只要花费足够的时间和努力，可以对任何人进行社会工程。千真万确，事实就是那么恐怖。但是这并不意味着没有希望，它意味着你的工作就是让恶意社会工程变得极为困难且耗时，这样大多数黑客就会放弃，转去摘取那些“低挂的果实”或追逐被落下的猎物。我知道这听起来很冷酷。如果大家都能阅读这本书并因此作出巨大的改变，我将十分欣慰，因为这样公司才会做到真正安全。然而，那就不是我们所处的世界了。

此番言论提出了一个非常严肃的问题。如果真的没有希望做得彻底安全，公司、员工、家庭以及我们每个人要如何来防护这个巨大的漏洞呢？只有公司开始意识到自己很容易被社会工程攻击，他们才会进行个人教育，了解攻击方法和保持警惕，并不断提醒他人。只有这样，我们才有希望在攻击前做好防御准备，或者至少不会后知后觉。

## 9.8　小结

作为全书的总结，我希望本书为你打开了认识社会工程世界的一扇窗，希望它能帮助你留意潜在的恶意攻击，帮助你对潜在的灾难形成并保持适度的恐惧。

同时，我也希望本书能帮助你保护你的公司、家庭、孩子、投资和生活。希望本书中的信息能让你体会到实现绝对安全和全面保护不是一件完全不可能的事。

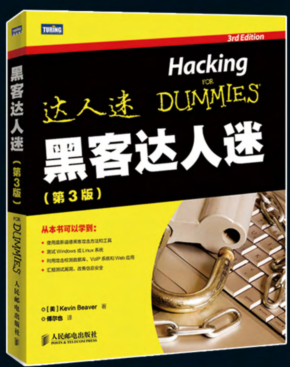
我的导师马蒂・阿哈罗尼曾在他的课上说过，坏人通常会得逞的原因在于他们付出了足够的时间和精力并且具有明确的动机。不要让生活妨碍安全。相反，也不要让过多的恐惧阻止你享受生活。

我希望通过应用本书中提到的原则，你能够提高自己读懂他人的能力，并能和周围的人进行更加有效的沟通。不要仅将它们运用在安全实践之中，要运用于生活的各个方面，这会改变你的生活。社会工程是一门真正的艺术。尽情享受它吧！

· 推 荐 阅 读 ·


iOS Hacker's Handbook
黑客攻防技术宝典
iOS实战篇


The Web Application Hacker's Handbook
黑客攻防技术宝典
Web实战篇（第2版）


3rd Edition
Hacking FOR DUMMIES
达人迷
黑客达人迷
（第 3 版）

“大部分恶意软件和客户端攻击中都会采用一些社会工程元素，用来欺骗用户以获得最终的控制权。你可以在技术上不断地为系统打补丁，但是没有一种补丁可以修复愚蠢、避免受骗。克里斯将为你揭示当今的攻击者是如何利用社会工程手法成功入侵的。本书将帮助你更好地了解和识破这种类型的攻击。”

——凯文•米特尼克，《欺骗的艺术》作者，世界知名社会工程专家

“克里斯•海德纳吉完成了社会工程领域的巅峰之作。通过细致的研究和丰富的实例，这本杰出的著作为你的企业甚至为你本人所面临的实际问题和风险提供了解决方案。这是真正的创新！”

——凯文•霍根，*The Science of Influence* 作者，美国最著名的说服心理学和人际沟通学专家

“本书并非黑客指南，因为他们已经知道怎样闯入系统并且每天都在研究新的方法。相反，克里斯•海德纳吉揭露了世界上最险恶的黑客、骗子以及社会工程人员的思路和方法，让我们有机会从黑暗的一面，也就是攻击者的视角来看系统安全与防护。”

——保罗•威尔逊，英国电视节目《骗术真相》主持人，亚太互联网络信息中心主席

不管你的安全设备有多么坚不可摧，防御流程有多么高效严密，安全系统中最薄弱、最容易入侵的环节却是人。专业的恶意社会工程人员似乎防不胜防，无法抵御，他们会运用人性的弱点攻破看似防护严密的系统。本书从攻击者的视角详细介绍了社会工程的所有方面，包括诱导、伪装、心理影响和人际操纵等，并通过凯文•米特尼克等社会工程大师的真实故事和案例加以阐释。内容包括黑客、间谍和骗子所使用的欺骗手法，以及防止社会工程威胁的关键步骤。

本书将帮助你：

- ◆学习社会工程人员采用的心理学原则及其运用方法
- ◆了解社会工程人员所精通的说服技巧
- ◆看清狡猾的骗子如何利用摄像头、GPS定位设备和来电显示行骗
- ◆知晓在网络上能够找到海量的个人信息
- ◆剖析真实世界中不可思议的社会工程实例

罪犯和恶意社会工程人员越来越猖獗，对企业和个人生活的攻击在不断增多。掌握了这些知识就像拥有了一盏明灯，可以照亮昏暗的角落，让你看清潜伏的恶意攻击者，并且采取有效的防御措施，使公司和个人事务免受攻击。

WILEY

Copies of this book sold without a Wiley sticker on the cover are unauthorized and illegal.

图灵社区：www.ituring.com.cn
新浪微博：@图灵教育 @图灵社区 @图灵新知
反馈/投稿/推荐信箱：contact@turingbook.com
热线：(010)51095186转600

分类建议 计算机/信息安全

人民邮电出版社网址：www.ptpress.com.cn

ISBN 978-7-115-33538-8

ISBN 978-7-115-33538-8
定价：59.00元

欢迎加入

# 图灵社区

## 最前沿的IT类电子书发售平台

电子出版的时代已经来临。在许多出版界同行还在犹豫彷徨的时候，图灵社区已经采取实际行动拥抱这个出版业巨变。作为国内第一家发售电子图书的IT类出版商，图灵社区目前为读者提供两种DRM-free的阅读体验：在线阅读和PDF。

相比纸质书，电子书具有许多明显的优势。它不仅发布快，更新容易，而且尽可能采用了彩色图片（即使有的书纸质版是黑白印刷的）。读者还可以方便地进行搜索、剪贴、复制和打印。

图灵社区进一步把传统出版流程与电子书出版业务紧密结合，目前已实现作译者网上交稿、编辑网上审稿、按章发布的电子出版模式。这种新的出版模式，我们称之为“敏捷出版”，它可以让读者以较快的速度了解到国外最新技术图书的内容，弥补以往翻译版技术书“出版即过时”的缺憾。同时，敏捷出版使得作、译、编、读的交流更为方便，可以提前消灭书稿中的错误，最大程度地保证图书出版的质量。

## 最方便的开放出版平台

图灵社区向读者开放在线写作功能，协助你实现自出版和开源出版的梦想。利用“合集”功能，你就能联合二三好友共同创作一部技术参考书，以免费或收费的形式提供给读者。（收费形式须经过图灵社区立项评审。）这极大地降低了出版的门槛。只要你有写作的意愿，图灵社区就能帮助你实现这个梦想。成熟的书稿，有机会入选出版计划，同时出版纸质书。

图灵社区引进出版的外文图书，都将在立项后马上在社区公布。如果你有意翻译哪本图书，欢迎你来社区申请。只要你通过试译的考验，即可签约成为图灵的译者。当然，要想成功地完成一本书的翻译工作，是需要有坚强的毅力的。

## 最直接的读者交流平台

在图灵社区，你可以十分方便地写作文章、提交勘误、发表评论，以各种方式与作译者、编辑人员和其他读者进行交流互动。提交勘误还能够获赠社区银子。

你可以积极参与社区经常开展的访谈、审读、评选等多种活动，赢取积分和银子，积累个人声望。

ituring.com.cn